IX kadencja

SEJM RZECZYPOSPOLITEJ POLSKIEJ

KANCELARIA SEJMU
Biuro Komisji Sejmowych

PEŁNY ZAPIS PRZEBIEGU POSIEDZENIA

■ **Komisji Obrony Narodowej**
(nr 17)
z dnia 17 listopada 2020 r.

Pełny zapis przebiegu posiedzenia

Komisji Obrony Narodowej (nr 17)

17 listopada 2020 r.

Komisja Obrony Narodowej, obradująca pod przewodnictwem posła **Michała Jacha (PiS)**, przewodniczącego Komisji, rozpatrzyła:

– informację Ministra Obrony Narodowej na temat bezpieczeństwa teleinformatycznego Sił Zbrojnych RP i systemu ochrony myśli technologicznej i technologii innowacyjnych na potrzeby pozyskiwanego sprzętu wojskowego dla Sił Zbrojnych RP.

– informację Ministra Obrony Narodowej na temat procesu formowania Wojsk Obrony Cyberprzestrzeni.

W posiedzeniu udział wzięli: **Wojciech Skurkiewicz** sekretarz stanu w Ministerstwie Obrony Narodowej, gen. bryg. **Karol Molenda** dyrektor Narodowego Centrum Bezpieczeństwa Cyberprzestrzeni oraz **Emilia Kunikowska** asystentka przewodniczącego Komisji Obrony Narodowej.

W posiedzeniu udział wzięli pracownicy Kancelarii Sejmu: **Kamil Strzępek** i **Jacek Zientarski** – z sekretariatu Komisji w Biurze Komisji Sejmowych.

Przewodniczący poseł Michał Jach (PiS):

Dzień dobry państwu. Otwieram 17. posiedzenie Komisji Obrony Narodowej. Stwierdzam przyjęcie protokołów 15. i 16. posiedzenia Komisji wobec niewniesienia do nich zastrzeżeń.

Witam przybyłych posłów i wszystkich, którzy uczestniczą w posiedzeniu w trybie online. Witam pana ministra Wojciecha Skurkiewicza, sekretarza stanu w Ministerstwie Obrony Narodowej. Witam pana generała brygady Karola Molendę, dyrektora Narodowego Centrum Bezpieczeństwa Cyberprzestrzeni. W trybie online są z nami przedstawiciele Departamentu Obrony Narodowej w Najwyższej Izbie Kontroli pan Mariusz Tupaj i pan Andrzej Dominikowski oraz pułkownik Mariusz Fryc z Biura Bezpieczeństwa Narodowego.

Jednocześnie informuję, że posłowie członkowie Komisji obecni na sali obrad Komisji głosują przy użyciu urządzenia do głosowania za pomocą legitymacji poselskiej, którą należy przyłożyć z lewej strony mikrofonu. Wówczas nie logują się w systemie komunikacji elektronicznej i nie używają tabletów.

W tej chwili przystąpimy do sprawdzenia kworum. Proszę państwa posłów o naciśnięcie jakiegokolwiek przycisku w celu potwierdzenia obecności na posiedzeniu. Dziękuję.

Głosowało 32 posłów. Stwierdzam kworum.

Informuję, że posiedzenie Komisji zostało zwołane przez panią marszałek Sejmu na podstawie art. 198j ust. 2 regulaminu Sejmu i będzie prowadzone z wykorzystaniem środków komunikacji elektronicznej umożliwiających porozumiewanie się na odległość. W związku z tym trybem procedowania nie ma możliwości rozszerzenia czy modyfikowania porządku dziennego dzisiejszego posiedzenia.

Tematem dzisiejszego posiedzenia jest w punkcie pierwszym informacja ministra obrony narodowej na temat bezpieczeństwa teleinformatycznego Sił Zbrojnych RP i systemu ochrony myśli technologicznej i technologii innowacyjnych na potrzeby pozyskiwanego sprzętu wojskowego dla Sił Zbrojnych Rzeczypospolitej Polskiej oraz w punkcie drugim informacja ministra obrony narodowej na temat procesu formowania Wojsk Obrony Cyberprzestrzeni.

Posiedzenie Komisji realizowane jest w formie wideokonferencji w systemie Whereby. Udział posłów oraz gości zewnętrznych ogranicza się do kliknięcia w link i połączenia z pokojem wideokonferencyjnym zgodnie z załączonymi instrukcjami. Transmisja na żywo dostępna jest w aplikacji do głosowania oraz na stronie sejmowej www.sejm.gov.pl. Chęć zabrania głosu zgłasza się poprzez mejla na adres kobn@sejm.gov.pl lub poprzez czat w aplikacji Whereby po zalogowaniu się do pokoju wideokonferencyjnego. Linka proszę używać w przypadku aktywnego uczestnictwa w posiedzeniu Komisji, na przykład chęci zabierania głosu w trakcie posiedzenia. W innym przypadku posiedzenie Komisji można śledzić z poziomu transmisji na stronie internetowej Sejmu.

Pragnę również przypomnieć, że na posiedzeniu Komisji 13 lutego tego roku przyjęliśmy propozycję prezydium Komisji w sprawie ograniczenia czasu wystąpień na naszych posiedzeniach. Pierwsze wystąpienie posła może trwać maksymalnie dziesięć minut, a każde kolejne pięć minut. Proszę o przestrzeganie tych limitów czasowych, żeby nasza dyskusja na posiedzeniach Komisji była uporządkowana i rzeczowa.

Zanim przejdziemy do informacji, pan minister Mroczek prosił o głos. Bardzo proszę, panie ministrze.

Poseł Czesław Mroczek (KO):

Dziękuję bardzo. Panie przewodniczący, panie ministrze, panowie generałowie, szanowni państwo, ja w kwestii formalnej, ponieważ – niestety – z przykrością muszę to odnotować, że nie odbyło się posiedzenie prezydium Komisji w związku z dzisiejszym posiedzeniem Komisji. Z uwagi na ten trudny czas, który mamy, który utrudniał prowadzenie normalnej pracy, proszę pana przewodniczącego o zwołanie w trybie zdalnym posiedzenia prezydium Komisji. I proszę, żeby pan zechciał powiedzieć w tej chwili albo przygotował taką odpowiedź na ewentualne posiedzenie prezydium Komisji, czy zamierza pan w najbliższym czasie zwołać posiedzenie Komisji Obrony Narodowej w sprawie udziału Ministerstwa Obrony Narodowej i sił zbrojnych w walce z pandemią koronawirusa, o co występowałem z wnioskiem na poprzednim posiedzeniu Komisji. Dziękuję bardzo.

Przewodniczący poseł Michał Jach (PiS):

Panie przewodniczący, panie ministrze, pragnę poinformować, że jutro o godz. 14:00 będzie posiedzenie prezydium, o czym powiadamialiśmy. Być może nie otrzymał pan powiadomienia SMS. Ja je otrzymałem. Jutro o godz. 14:00 mamy posiedzenie prezydium, na którym będziemy mogli…

Poseł Czesław Mroczek (KO):

Szybkie załatwienie sprawy. Dziękuję bardzo.

Przewodniczący poseł Michał Jach (PiS):

Można? Tak jest. W takim razie bardzo proszę pana ministra o przedstawienie informacji dotyczącej punktu pierwszego, czyli bezpieczeństwa.

Sekretarz stanu w Ministerstwie Obrony Narodowej Wojciech Skurkiewicz:

Panie przewodniczący, mam gorącą prośbę – jeśli państwu posłom nie będzie to przeszkadzało – żebyśmy mogli obydwa punkty rozpatrywać jednocześnie, bo one wiążą się ze sobą.

Przewodniczący poseł Michał Jach (PiS):

Bardzo proszę.

Sekretarz stanu w MON Wojciech Skurkiewicz:

Szanowni państwo, panie przewodniczący, Wysoka Komisjo, na przestrzeni lat obserwujemy rozwój informatyzacji praktycznie wszystkich obszarów naszego życia. Obszar IT jest coraz mocniej obecny nie tylko w gałęziach przemysłu, ale również w naszym życiu, praktycznie na każdym kroku. Powszechne jest oczekiwanie, że organy państwa będą w związku z tym zapewniać pewien poziom bezpieczeństwa użytkowników tego obszaru. To, że powszechność dostępu jest tak szeroka, niesie za sobą również całe mnóstwo zagrożeń i nienotowanych wcześniej wyzwań dla szeroko pojętego bezpieczeństwa. Nie tylko bezpieczeństwa w aspekcie wewnętrznym, ale również bezpieczeństwa szeroko rozumianego. Można tutaj mówić wręcz o bezpieczeństwie międzynarodowym.

Postępująca cyfryzacja systemów przetwarzania informacji wprowadza nowe rodzaje zagrożeń związanych z możliwością ich niewłaściwego wykorzystywania. Wydaje się to o tyle istotne, że chociażby Federacja Rosyjska, która jest oceniana jako główne źródło zagrożeń w naszej części Europy, od 2000 r. jednoznacznie wskazuje sferę działań w cyberprzestrzeni jako element wojny informacyjnej. W oficjalnych dokumentach jest ona określana jako sfera działań związanych z kształtowaniem, tworzeniem, przekształcaniem przekazu, wykorzystywaniem i przechowywaniem informacji wpływających na świadomość indywidualną i społeczną, a także infrastrukturę informacyjną i wprost na informacje.

Co więcej, w Rosji już od ponad dwudziestu lat kształci się specjalistów w obszarze bezpieczeństwa informacyjnego, przy czym zasilają oni nie tylko służby specjalne i siły zbrojne, ale również formacje polityczne oraz aparat i administrację państwową. Federacja Rosyjska wielokrotnie wykorzystywała działania w cyberprzestrzeni jako działania wspierające dla prowadzonych działań militarnych. Warto tutaj wspomnieć chociażby 2008 r. i wojnę w Gruzji czy 2014 r. i agresję na Ukrainę, gdzie ten obszar był bardzo szeroko wykorzystywany.

Z uwagi na wyżej wymienione uwarunkowania oraz nowego rodzaju zagrożenia wynikające z coraz szerszego wykorzystania oraz coraz szerszej obecności technik informatycznych Sojusz Północnoatlantycki już w 2014 r. uznał atak w cyberprzestrzeni za jeden z rodzajów agresji, który może stanowić podstawę do wprowadzenia w życie mechanizmów obronnych opisanych w art. 5 Traktatu północnoatlantyckiego. Taki stan rzeczy został również potwierdzony w 2016 r. podczas szczytu NATO w Warszawie, na którym oficjalnie uznano cyberprzestrzeń jako jedną z domen działań operacyjnych. To z kolei zrodziło konieczność opracowania przez NATO konkretnych struktur sojuszu, strategii ich funkcjonowania oraz realizacji przez nie działań o charakterze operacyjnym w wyżej wymienionej domenie cyfrowej.

Podczas tego szczytu ustalono, że cyberprzestrzeń jest aktualnie strefą zainteresowań i wpływów, w której – w zakresie militarnym, jak również pozamilitarnym – podejmowane są działania, funkcje i operacje niezbędne do wykonywania misji i sprawowania kontroli nad przeciwnikiem w celu osiągnięcia pożądanych efektów. Każde państwo powinno samodzielnie rozwijać zdolności defensywne własnych sił zbrojnych w tym obszarze. Osiągnięcie wymaganego poziomu do działań w domenie cyberprzestrzeni stanowi Cyber Defense Pledge, czyli jest obowiązkiem wszystkich członków Sojuszu Północnoatlantyckiego. W celu zwiększenia zdolności do realizacji zadań mających zapewnić odpowiedni poziom bezpieczeństwa narodowych systemów IT, w resorcie obrony narodowej w ostatnich latach podejmowane były i są liczne przedsięwzięcia natury informacyjnej, promocyjnej, organizacyjnej i szkoleniowej.

Do najważniejszych z nich z pewnością można zaliczyć konsolidację zasobów resortu obrony narodowej w zakresie struktur odpowiedzialnych za zapewnienie bezpieczeństwa teleinformatycznego i cyberbezpieczeństwa, obejmującą utworzenie Narodowego Centrum Bezpieczeństwa Cyberprzestrzeni na bazie Narodowego Centrum Kryptologii oraz Inspektoratu Informatyki. Znacząco zwiększono nabór studentów wojskowych, w szczególności studentów Wojskowej Akademii Technicznej, w specjalnościach informatyka oraz kryptologia i cyberbezpieczeństwo. W latach 2020–2022 zwiększono limit przyjęć na te kierunki odpowiednio do 107 i 116 studentów. W 2018 r. uruchomiono program CYBER.MIL, którego jednym z głównych celów – poza integrowaniem środowiska cyberbezpieczeństwa resortu obrony narodowej – jest przyciągnięcie do struktur resortu obrony narodowej, a szczególnie do sił zbrojnych, młodych i zdolnych specjalistów z tego obszaru.

Podjęto realizację programu operacyjnego „Bezpieczeństwo w cyberprzestrzeni i wsparcie kryptologiczne", obejmującego budowę kluczowych z punktu widzenia bezpieczeństwa państwa zdolności Sił Zbrojnych Rzeczypospolitej Polskiej do realizacji zadań z zakresu ochrony i obrony cyberprzestrzeni oraz rozwoju narodowych rozwiązań kryptologicznych. Podjęto decyzję o utworzeniu Wojsk Obrony Cyberprzestrzeni. Powołano pełnomocnika ministra obrony narodowej do spraw utworzenia Wojsk Obrony Cyber-

przestrzeni. W dniu 12 września 2019 r. zatwierdzono koncepcję organizacji i funkcjonowania Wojsk Obrony Cyberprzestrzeni.

Należy zaznaczyć, że ochrona i obrona cyberprzestrzeni Rzeczypospolitej Polskiej wymaga systemowych, skorelowanych działań na możliwie najwyższym poziomie decyzyjnym oraz jednoznacznych uregulowań prawnych, zarówno na poziomie resortowym, jak i ogólnokrajowym. Działania w sferze wojskowej w tym obszarze, w szczególności polegające na sformowaniu Wojsk Obrony Cyberprzestrzeni, należy traktować jedynie jako budowę stabilnego fundamentu ogólnokrajowego systemu obrony cyberprzestrzeni oraz stworzenie procedur i narzędzi umożliwiających realizację przez ministra obrony narodowej ustawowych zadań w ramach krajowego systemu cyberbezpieczeństwa. Panie przewodniczący, szanowni państwo, to tyle, jeżeli chodzi o sam wstęp. Myślę, że pan generał Molenda, szef Narodowego Centrum Bezpieczeństwa Cyberprzestrzeni, przedstawi teraz prezentację i uzupełni kilka kolejnych rzeczy.

Przewodniczący poseł Michał Jach (PiS):

Bardzo proszę, panie generale.

Dyrektor Narodowego Centrum Bezpieczeństwa Cyberprzestrzeni gen. bryg. Karol Molenda:

Dziękuję bardzo. Panie przewodniczący, Wysoka Komisjo, jest mi niezmiernie miło, że mam możliwość omówić ten temat. Z jednej strony jest on mi bardzo bliski, bo przez całe moje zawodowe życie zajmuję się bezpieczeństwem. Wcześniej nie było słowa „cyber", więc było to „information assurance", a więc bezpieczeństwo informatyczne. Później pojawiły się słowa „cyber", „cyberprzestrzeń" i wszystkie aspekty z tym związane. A od 5 lutego 2019 r. mam przywilej bycia pełnomocnikiem ministra obrony narodowej do spraw utworzenia Wojsk Obrony Cyberprzestrzeni, a zarazem od marca zeszłego roku dyrektorem Narodowego Centrum Bezpieczeństwa Cyberprzestrzeni, na bazie którego powstają te wojska.

Postaram się dzisiaj wprowadzić państwa w ten świat. Przy założeniu, że czasami obraz pokazuje więcej niż tysiąc słów, mam opracowaną prezentację, która pozwoli w sposób graficzny przedstawić pewne etapy, które realizujemy. Niestety, ubolewam nad tym, że koncepcja jest dokumentem niejawnym. Cała koncepcja utworzenia Wojsk Obrony Cyberprzestrzeni ma charakter niejawny. Stąd pozwoliłem sobie zaadresować do państwa dodatkową informację. Informację niejawną, z którą oczywiście mogą się państwo zapoznać. Z racji trybu, w którym odbywamy to spotkanie, nie będę w stanie zaprezentować w dniu dzisiejszym pełnej informacji, którą chciałbym podać, chociażby odnośnie do liczb, danych statystycznych i incydentów, o których jest mowa w tym dokumencie.

Natomiast będę chciał państwu przedstawić wyciąg z tej koncepcji oraz informacje o zadaniach, które zrealizowaliśmy w ciągu ostatniego roku, a nawet półtora roku. Pan minister już wspomniał, że postęp technologiczny, wzrost zagrożeń, które istnieją w cyberprzestrzeni, sposób postrzegania cyberprzestrzeni – wszystko to zaowocowało tym, że ta przestrzeń została zauważona jako przestrzeń oddziaływania potencjalnych adwersarzy i prowadzenia różnych działań i operacji. Różnych operacji, w tym operacji ofensywnych, mających na celu zakłócenie funkcjonowania systemów, jak również wyprowadzenie czy pozyskanie informacji, które są w tych systemach gromadzone i przetwarzane. Jak już powiedziano, NATO też zauważyło ten problem. Chociażby na szczycie w Warszawie w 2016 r. cyberprzestrzeń została zdefiniowana jako kolejna domena operacyjna, do obrony której siły zbrojne muszą się przygotować tak samo jak do bronienia lądu, morza, powietrza czy do działań związanych z kosmosem.

Jest to o tyle ciekawe, że cyberprzestrzeń jest jedyną z domen całkowicie zbudowaną przez człowieka. Czyli ona codziennie się zmienia. Nie jest tak jak z pozostałymi domenami, które mają pewne właściwości. Dla przykładu powiem, że jeżeli samolot zostanie zestrzelony w powietrzu, to właściwości powietrza są niezmienne. Kolejne statki powietrzne mogą tam latać. Jeżeli na morzu zostanie zatopiony okręt, morze ma te same parametry. Tu się nic nie zmienia. Natomiast, jeżeli pewne działania odbywają się w cyberprzestrzeni, użytkownicy, administratorzy albo twórcy, czyli osoby, które odpo-

wiadają za te systemy, korygują swoje urządzenia i aktualizują swoje aplikacje. Czyli cyberprzestrzeń cały czas się zmienia.

Co więcej, rozwój technologiczny i fakt, że w cyberprzestrzeni pojawiają się nowe funkcjonalności, nowe urządzenia czy nowe zasoby, odkrywa tę cyberprzestrzeń na kolejne zagrożenia. Czyli tak naprawdę jest to niekończąca się ochrona cyberprzestrzeni. To jest niekończący się proces. To nie jest stan. To jest proces. Oczywiście cyberprzestrzeń jest strefą zainteresowania i wpływów. Z jednej strony mówi się o efektach, czyli o działaniach w cyberprzestrzeni. Prowadzenie operacji w cyberprzestrzeni ma na celu doprowadzenie do pewnych efektów czy uzyskanie pewnych efektów. Oczywiście to mogą być efekty związane z działaniami operacyjnymi – defensywnymi, ale również ofensywnymi.

Co więcej, prowadzona jest działalność rozpoznawcza. Poszczególne kraje – i nie tylko – rozpoznają właściwości systemów i sieci teleinformatycznych przeciwnika bądź innych krajów, tak żeby mogły wykorzystać tę wiedzę do swego targetingu. Jak już wspomniano, w ramach definiowania domeny cyberprzestrzennej przez NATO jako kraj, jako członek NATO podjęliśmy pewne zobowiązanie, które zostało sformułowane jako Cyber Defense Pledge. To zobowiązanie nakłada na nas obowiązek zbudowania kompetencji do obrony i prowadzenia operacji w cyberprzestrzeni. Operacje w cyberprzestrzeni możemy podzielić na kilka typów. Ogólny podział może być na cyberops i infoops. Jeżeli mówimy o cyberops, mówimy o operacjach czy działaniach z wykorzystaniem cyberprzestrzeni, z wykorzystaniem systemów, czyli z przełamywaniem zabezpieczeń, z przełamywaniem właściwości sprzętu i aplikacji w celu dostania się do systemu. Operacje infoops to rodzaj operacji informacyjnych z wykorzystaniem cyberprzestrzeni. Dla przykładu są to na przykład sławetne fake newsy, portale społecznościowe czy strony, na których zostaje zamieszczona nieprawdziwa informacja mogąca wpływać na postawy użytkowników. Często przeciwnicy prowadzą operacje w cyberprzestrzeni w taki sposób, że wykorzystują elementy socjotechniki, czyli działań informacyjnych, żeby przekonać użytkownika do tego, żeby zrobił coś w ramach działań cyberops. Dla przykładu dobrym typem ataku, który w większości przypadków jest bardzo skuteczny, jest atak phishingowy. Ma on na celu na przykład wysłanie mejla podszywającego się pod kogoś, pod zaufanego nadawcę, i przekonującego do tego, żeby coś zrobić – kliknąć na link, podać swoje poświadczenia, podać swój login, podać swoje hasło – by w ten sposób pozyskać pewne informacje. To jest jedna z możliwości działania.

Co zrobiliśmy w ciągu ostatniego roku? Przede wszystkim określiliśmy czy sprawdziliśmy, czym dysponujemy w siłach zbrojnych, jakie mamy zasoby w zakresie informatyki, działań w cyberprzestrzeni oraz kryptologii. Zauważyliśmy, że część zasobów jest rozrzucona po różnych instytucjach, po różnych jednostkach organizacyjnych.

Dla przykładu podam, że Inspektorat Informatyki odpowiadał za proces informatyzacji i utrzymanie systemów teleinformatycznych w resorcie obrony narodowej. Jego głównym zadaniem była funkcjonalność tych systemów. Głównym celem nie było bezpieczeństwo. Wiadomo, że jest to zawsze wyścig pomiędzy funkcjonalnością a bezpieczeństwem. Czym coś jest bardziej bezpieczne, tym jest mniej funkcjonalne. I na odwrót. Jeżeli jednostka istnieje tylko po to, żeby system działał, jeżeli żadnym z priorytetów tego inspektoratu nie było bezpieczeństwo, to powiedzmy sobie, że bezpieczeństwo systemów, które były budowane i utrzymywane, nie było na najwyższym poziomie. Z drugiej strony Narodowe Centrum Kryptologii było typową jednostką, która dbała o bezpieczeństwo. Była wręcz przeznaczona do tego, żeby tworzyć szyfratory bądź monitorować sieci. W tym momencie były dwie jednostki na tym samym poziomie, a każda z nich miała inne zadania. Analizując możliwości i nasze potrzeby, doszliśmy do przekonania, że należy skonsolidować zasoby, którymi dysponujemy. Na bazie Inspektoratu Informatyki i Narodowego Centrum Kryptologii powstało Narodowe Centrum Bezpieczeństwa Cyberprzestrzeni jako jednostka, która konsoliduje te zasoby.

W tym momencie dyrektor NCBC ma za zadanie budowanie i utrzymanie systemów teleinformatycznych. To już jest jego zadaniem, żeby te systemy były utrzymywane, zarządzane, ale też budowane – bo mówimy o nowych – w sposób uwzględniający z jednej strony bezpieczeństwo, jak również ich funkcjonalność. Czyli powstało Narodowe Centrum Bezpieczeństwa Cyberprzestrzeni. W podporządkowaniu Narodowego Centrum

Bezpieczeństwa Cyberprzestrzeni jest sześć regionalnych centrów informatyki, czyli jednostek, które odpowiadają za swój region, jeżeli chodzi o utrzymanie stacjonarnych systemów teleinformatycznych resortu obrony narodowej. Oprócz tego jest jednostka Centrum Zasobów Cyberprzestrzeni Sił Zbrojnych, która jest naszą jednostką logistyczną.

W resorcie obrony narodowej nie ma komputera, laptopa ani tabletu, ani innego elementu infrastruktury teleinformatycznej, który nie zostałby zakupiony lub skonfigurowany przez NCBC lub jednostki bezpośrednio mu podległe. Oprócz tych jednostek IT mamy również Centrum Operacji Cybernetycznych, czyli jednostkę, na bazie której to rozbudowujemy i na bazie której będziemy też budować przyszłe Wojska Obrony Cyberprzestrzeni. Oczywiście naszą siłą są kadry i intelekt tych osób. Czyli tak naprawdę nie ilość, tylko jakość. Naszym głównym zadaniem jest pozyskanie właściwych osób, by dołączyły do naszych zespołów, by służyły. Byłoby najlepiej, gdyby założyły mundur.

Oczywiście pozyskujemy żołnierzy, ale również pracowników wojska, czyli cywili, bo nie we wszystkich operacjach potrzebni są żołnierze. Poza tym ten proces pozwala na pewną elastyczność przy zarządzaniu projektami. Jak już wspomniał pan minister, znacznie zwiększyliśmy nabór. Został zwiększony nabór do dwóch kluczowych uczelni wojskowych, które kształcą w tym zakresie. Oczywiście jest to Wojskowa Akademia Techniczna, w której chociażby w latach 2015 i 2016 na elektronice było 84 i 97 osób. W chwili obecnej na rok 2020/2021 są to 222 osoby – 222 podchorążych. Na informatyce z 47 osób w 2015 r. liczba studentów wzrosła do 107 w 2021 r. Na kryptologii i cyberbezpieczeństwie z 15 osób w 2015 r. liczba studentów wzrosła do 116 osób w 2021 r. To jeżeli chodzi o Wojskową Akademię Techniczną.

Równocześnie zwiększono limity przyjęć w Akademii Marynarki Wojennej do 22 podchorążych na kierunku informatyka. Jednocześnie w tym roku zostaje uruchomiony kierunek informatyka w Akademii Wojsk Lądowych we Wrocławiu. Jeżeli chodzi o nasze kolejne inicjatywy, zauważyliśmy – nie chciałbym powiedzieć, że studenci są za starzy – że należy zaadresować nasze potrzeby do młodszej młodzieży. Dlatego z jednej strony powstało Wojskowe Ogólnokształcące Liceum Informatyczne przy WAT, które co roku przyjmuje 50 uczniów. Teraz jest już drugi rok funkcjonowania tego liceum. Uważam, że ono jest sukcesem, bo na pierwszy rok zgłosiło się ponad 500 kandydatów. Młodzież, która tam jest, ma przeznaczony dla niej autorski kierunek związany z cyberbezpieczeństwem i informatyką. Część nauczycieli to wykładowcy z Wojskowej Akademii Technicznej. Jestem przekonany, że jeżeli te osoby zdecydują się pozostać i dołączyć do Wojskowej Akademii Technicznej jako studenci podchorążowie, to będzie to bardzo mocny zasób, jeżeli chodzi o przyszłych podchorążych, którzy mają wyrównaną wiedzę.

Kolejny program, który został zainicjowany w tym roku, to program „CYBER.MIL z klasą”. Program ma na celu, żeby w każdym województwie była jedna szkoła średnia, która będzie miała autorski program w zakresie cyberbezpieczeństwa. Co więcej, nie tylko ten program jest opracowany przez nas, ale szkoła średnia dostaje środki finansowe na infrastrukturę i na prowadzenie zajęć w tej klasie. Klasa nie może mieć więcej niż 15 uczniów. Jest to typowa klasa przeznaczona do programu autorskiego.

Jest również nadzór merytoryczny. Jednostki, o których wspominałem, czyli regionalne centra informatyki podległe NCBC, mają za zadanie sprawowanie nadzoru merytorycznego nad tymi szkołami. Mają tam po prostu być obecne na co dzień, wspierać i w pewien sposób wpływać na to – oczywiście nie będzie takiego przymusu – żeby uczniowie rozważyli po liceum naukę na uczelniach wojskowych na kierunkach informatyka lub cyberbezpieczeństwo.

Oczywiście zachęcam do tego, żeby chwalić się wszystkimi naszymi jawnymi inicjatywami. Chwalimy się tym. To też w pewien sposób wpływa na budowanie pozycji Narodowego Centrum Bezpieczeństwa Cyberprzestrzeni. Jestem przekonany, że w ciągu roku udało się wypracować nie tylko nazwę, ale to, jak to centrum jest postrzegane przez specjalistów na rynku. Coraz więcej osób czy specjalistów, którzy zajmują się bezpieczeństwem cyberprzestrzeni, docenia nasze kompetencje i nas zauważa.

Ale to też wynika z tego, że jesteśmy obecni na wielu branżowych konferencjach. Praktycznie w chwili obecnej jesteśmy współorganizatorem części z nich. Jesteśmy jedną z jednostek, które współorganizują takie konkursy jak capture the flag. Tam można

wyłapać najlepszych uczestników takich konferencji. To też buduje wizję naszego centrum jako centrum eksperckiego.

Kolejną inicjatywą jest chociażby Letnia Szkoła Cyberbezpieczeństwa. Jest Letnia Szkoła Cyberbezpieczeństwa i Zimowa Szkoła Cyberbezpieczeństwa. Są to takie konferencje, tygodniowe spotkania, które pomagają w wyrównywaniu wiedzy w zakresie cyberbezpieczeństwa. Wśród zaproszonych gości często bywają osoby, które odpowiadają za kluczowe aspekty bezpieczeństwa chociażby w administracji państwowej.

Kolejna inicjatywa to uruchomienie studiów MBA z zakresu cyberbezpieczeństwa w Wojskowej Akademii Technicznej. Teraz jest to już drugi rok tych studiów. Faktycznie te studia cieszą się coraz większym zainteresowaniem. Są one wręcz zauważane nawet poza granicami Polski. Często jestem pytany o możliwości uczestnictwa w zajęciach na tym kierunku studiów podyplomowych. Są też inne inicjatywy. Dla przykładu powiem, że mamy konkurs na najlepszą pracę doktorską i na najlepszą pracę magisterską z zakresu informatyki i cyberbezpieczeństwa. W chwili obecnej trwa druga edycja tego konkursu. W grudniu będą wręczane nie tylko wyróżnienia dla najlepszych prac, ale również nagrody finansowe.

Dalej pozyskiwanie kadr. Wspominałem o programie „CYBER.MIL z klasą”. Mamy też Legię Akademicką, która cieszy się bardzo dużym zainteresowaniem. W tym roku mieliśmy drugą edycję tego projektu. Jest to możliwość, żeby studenci z całej Polski w okresie wakacji mogli odbyć przeszkolenie wojskowe i uzyskać stopień kaprala rezerwy. W tym roku skorzystało z tego ponad 77 studentów z kierunków informatyki i cyberbezpieczeństwa, którzy odbyli szkolenie prowadzone przez NCBC na kierunku cyberbezpieczeństwo. Dzięki temu mogą być rozważani jako przyszli żołnierze w naszych strukturach. Powiem, że w tym roku to cieszyło się ogromnym zainteresowaniem. Chętnych było ponad 350 studentów. Wybraliśmy 77 najlepszych. Z tego już w tym roku zgłosiło się kilku żołnierzy rezerwy, którzy są absolwentami studiów i chcą dołączyć jako żołnierze do NCBC.

Sytuacja związana z COVID-em doprowadziła do braku możliwości bezpośredniego kontaktu tak częstego jak w przeszłości. Nie jesteśmy obecni fizycznie na konferencjach, na których moglibyśmy pozyskiwać kadrę. Oczywiście utrudniony jest również kontakt z potencjalnymi kandydatami. Dlatego przeszliśmy do strefy cyfrowej. Uruchomiliśmy infolinię przeznaczoną dla kandydatów do Narodowego Centrum Bezpieczeństwa Cyberprzestrzeni, gdzie można uzyskać wszelkie odpowiedzi. Oczywiście rozmowy rekrutacyjne z kandydatami prowadzimy też za pomocą środków komunikacji internetowej. Co więcej, doprowadziliśmy do takiej sytuacji, że kandydaci zdają test. To też ma dla nas znaczenie, żeby wybrać najlepszych.

Powiem, że zainteresowanie też jest bardzo duże. Poprosiłem o statystyki. W 2019 r. łącznie cywili, którzy do nas trafili, było 958. A w 2020 r. do chwili obecnej – 1330. Czyli w sumie mamy 2288 cywili. W tej grupie odbyliśmy 726 rozmów kadrowych. Oczywiście wiadomo, że nie w każdej rozmowie jesteśmy w stanie ocenić potencjalnego kandydata. Dlatego kandydaci dostają test do zrobienia. Dostają 30 pytań, na odpowiedź jest 30 minut, w sposób zdalny. Klikając na link, uruchamiają test przeznaczony dla danego kandydata. Oczywiście to też pozwala nam na pewną ocenę wiedzy, bo test jest przekrojowy. Nie jest zbyt trudny, ale daje nam pewne pojęcie o tym, czy jesteśmy zainteresowani kandydatem, który uzyskał dany wyniki, czy dalej jesteśmy nim zainteresowani. Zauważyłem, że od kiedy pojawił się ten test, aspiracje finansowe niektórych kandydatów zeszły w dół. To, że ktoś jest magistrem inżynierem, nie znaczy za każdym razem, że ma taką wiedzę, która przydałaby się nam.

Kolejna rzecz to usprawnienie systemu rekrutacji. Na polecenie ministra obrony narodowej sposób rekrutacji został wprowadzony w XXI w. Opracowaliśmy witrynę zostanzołnierzem.pl, na której w sposób zdalny można zgłosić swój akces i otrzymać dokumenty do tego niezbędne. Jednocześnie te dane trafiają do właściwej wojskowej komendy uzupełnień. W chwili obecnej jesteśmy w przededniu uruchomienia aplikacji Zostań Żołnierzem na urządzenia mobilne – iOS i Android. Będzie możliwość zrobienia tego samego co w witrynie, a jednocześnie będzie można śledzić swoje postępy w procesie rekrutacji. Oczywiście obydwie aplikacje i witryna są przeznaczone dla całych sił zbroj-

nych. Natomiast liczę na to, że to przyspieszy nam działania dotyczące Wojsk Obrony Cyberprzestrzeni.

I pewna wisienka na torcie. Myślę, że w dniu dzisiejszym już można to zakomunikować, chociaż tak naprawdę dopiero w dniu jutrzejszym o godz. 12:00 – zachęcam do oglądania relacji – zostanie oficjalnie zainaugurowane Eksperckie Centrum Szkolenia Cyberbezpieczeństwa. Jest to nowo utworzona jednostka, która powstała 2 listopada. Jutro jest oficjalna inauguracja. Natomiast od 9 listopada to centrum już szkoli. Zauważyliśmy, że niezbędny jest nam nie tylko nabór tych ludzi, ale także ciągłe szkolenie ich umiejętności i wiedzy. Jak każdy żołnierz w poszczególnych rodzajach wojsk, tak i nasi żołnierze potrzebują mieć poligon, na którym mogą podnosić swoje kwalifikacje. Eksperckie Centrum Szkolenia Cyberbezpieczeństwa będzie właśnie takim miejscem. Już jest takim miejscem, a będzie wzmacniało swoje kompetencje.

Już są określone ścieżki szkoleniowe dla naszych poszczególnych żołnierzy i pracowników wojska, w zależności od specjalności czy zadań, które będą realizowali, żeby w sposób ciągły mogli podnosić swoje umiejętności. Ale również żeby zapewnić szkolenia autorskie i możliwość dzielenia się wiedzą chociażby z incydentów, po incydentach. Nie ma takich szkoleń na rynku prywatnym. Często jest to wiedza oznaczona jako informacja niejawna. Ale nigdzie nie ma tego, co będzie u nas pewnym novum, czyli możliwości zgrywania zespołów. Może nie jest tak, że nie ma tego nigdzie. Jest taka możliwość w Fort Gordon w Stanach Zjednoczonych. Jest tam również centrum eksperckie, które zgrywa tak armię amerykańską. Skorzystaliśmy z doświadczeń naszego partnera i chcemy nie tylko szkolić nasze zespoły osobowe, ale również je zgrywać, bo to jest bardzo istotne. Zespół ma być zgrany. W ramach takich ćwiczeń można wyszukiwać liderów, którzy wezmą na siebie odpowiedzialność za funkcjonowanie takiego zespołu. Stąd eksperckie centrum i jego inauguracja w dniu jutrzejszym. Natomiast tak naprawdę zaczęło ono swoje funkcjonowanie już w tym miesiącu.

Co więcej, już zostało zauważone, nawet za granicą. Ta informacja przeszła do naszych partnerów. Część naszych partnerów widzi ewentualną możliwość przysyłania i – oczywiście odpłatnego – szkolenia swoich żołnierzy w tym centrum. To jest pewne novum, którego tak naprawdę w Europie nie ma. Jest eksperckie Centrum Doskonalenia Cyberobrony NATO w Tallinie. Natomiast przepustowość tego centrum, jeżeli chodzi o szkolenie, to dwie osoby na kraj. Polskie siły zbrojne potrzebują przeszkolić kilka tysięcy osób. Proces szkolenia w tamtym centrum byłby niemożliwy do zaakceptowania, nie mówiąc już o kosztach. A tutaj możemy korzystać z naszych doświadczeń, z naszych zasobów eksperckich, którymi dysponujemy. Jestem przekonany, że jest to inicjatywa, która będzie korzystnie odebrana i która zafunkcjonuje. Nasze działania są finansowane w ramach programu operacyjnego „Bezpieczeństwo w cyberprzestrzeni i wsparcie kryptologiczne".

Co więcej zrobiliśmy? Oczywiście pracownicy cywilni to jedno, ale są również żołnierze. Decyzją ministra obrony narodowej został przyznany dodatek o charakterze stałym dla żołnierzy wykonujących zadania w zakresie cyberbezpieczeństwa i informatyki. Oczywiście w zależności od ich wiedzy i umiejętności ten dodatek może wynosić od 450 zł do 2100 zł. Jako dodatek stały, czyli 10% za każdy rok, jest on dodawany do emerytury, co już spowodowało dość korzystne zainteresowanie nie tylko pracą, ale także służbą. Jednocześnie w zależności od zaangażowania żołnierzy w realizację zadań dyrektor NCBC ma możliwość przyznania od 100% do 620% jednorazowego dodatku raz w roku, w zależności od osiągnięć danego żołnierza i jego zaangażowania. Jestem przekonany, bo już to widzę, że to też pozytywnie wpływa na realizację tych zadań.

Współpraca. Oczywiście współpracujemy w ramach reagowania na incydenty komputerowe, bo w ramach NCBC funkcjonuje też CSIRT MON, czyli zespół reagowania na incydenty komputerowe Ministerstwa Obrony Narodowej. Oczywiście żeby wyjaśniać incydenty i koordynować ich obsługę, niezbędna jest współpraca ze służbami w tym zakresie, również z CERT NASK, a także z uczelniami, które mogą zasilać nas kadrowo. To jest kolejny program, który został uruchomiony w tym tygodniu. Mam nadzieję, że więcej informacji na ten temat pojawi się już w piątek. Postaram się, żeby jeszcze w tym tygodniu pojawiło się więcej informacji.

Nowy autorski program to „Cyfrowi ambasadorzy NCBC". Zauważyliśmy, że nie jesteśmy w stanie być obecni na wszystkich uczelniach, na których chcielibyśmy być obecni. Natomiast jesteśmy skorzy, żeby na tych uczelniach, na których nam zależy, znaleźć osoby – wyróżniających się studentów – które mogłyby być naszymi ambasadorami, naszymi przedstawicielami i budować obraz centrum, ale też wojska oraz zachęcać i informować o inicjatywach. Jest bardzo duże zainteresowanie. Jestem przekonany, że bardzo dużo uczelni przystąpi do programu. Pierwsza była Wojskowa Akademia Techniczna, ale jest wiele innych, które już chcą zgłosić swoich studentów do programu „Cyfrowy ambasador NCBC". Mam nadzieję, że dzięki temu współpraca będzie się intensyfikowała.

Oczywiście współpraca międzynarodowa jest również bardzo istotna. Mamy podpisane porozumienie z naszymi partnerami, czyli z US Cyber Command reprezentowanym przez dowództwo w Europie. W zakresie cyberbezpieczeństwa jest to bardzo dobre, bardzo merytoryczne porozumienie, ale także bardzo dobra współpraca. Nasze zespoły wymieniają się informacjami o zagrożeniach, ale też uczą się od siebie nawzajem.

Podpisana jest również współpraca z agencją NCI Agency z NATO, w ramach której funkcjonuje NATO Cyber Security Centre, czyli wcześniejszy NCSIRT – zespół reagowania na incydenty komputerowe w sieciach NATO. Mamy ustalone zakresy wymiany informacji i funkcjonowanie punktów przez 24 godziny na dobę, 7 dni w tygodniu, 365 dni w roku. Nasze centra operacyjne NCBC także pracują w trybie 24 godziny na dobę.

Jeśli chodzi o kolejne współprace i kolejnych partnerów międzynarodowych, to rozmawiamy z nimi. Bardzo nas interesują. Osobiście nie chodzi mi o to, żeby mieć bardzo dużo porozumień, tylko o to, żeby współpraca międzynarodowa, która będzie zainicjowana, była współpracą win-win. Czyli nie tylko dajemy, ale także otrzymujemy. Staramy się takich partnerów poszukiwać w Grupie Wyszehradzkiej i wśród innych cyberdowództw w NATO. Muszę przyznać, że jest dość duży odzew w tym zakresie. Natomiast czas pokaże, którzy partnerzy będą tymi, którzy się sprawdzą.

Jak zauważono, jednym z zadań mojego zespołu jako pełnomocnika ministra obrony narodowej do spraw utworzenia Wojsk Obrony Cyberprzestrzeni było określenie koncepcji funkcjonowania czy budowania tych wojsk. Bardzo zależało nam na tym, żeby skrócić czas ich formowania. Dla przykładu powiem, że bardzo ambitny plan, który określiliśmy, dotyczy zbudowania zdolności do działania w pełnym spektrum cyberprzestrzeni w ciągu 4–5 lat. Jest to o tyle ambitny plan, że chociażby Amerykanie budowali swoje zdolności przez 11 lat. Mam nadzieję, że fakt wymiany informacji z naszymi partnerami, w tym z Amerykanami, o czym wspominałem wcześniej, pozwoli nam na przyspieszenie. Z Amerykanami wymieniamy się też informacjami o błędach, które popełnili w trakcie budowania swoich zdolności. Chodziło nam o to, żeby przyspieszyć i skrócić ten czas.

Oczywiście konieczna jest maksymalna efektywność tego procesu tworzenia, czyli minimalny koszt w stosunku do efektu, który zadeklarowaliśmy. Ta koncepcja zakładała pewną ewolucję zamiast rewolucji. Nie budowaliśmy wszystkiego od początku. Dokonaliśmy przeglądu tego, czym dysponujemy, i określiliśmy ścieżki, jak dojść do efektów końcowych. Tak też bywa. To jest przykład chociażby z modelu amerykańskiego, w którym nie pozyskiwano czy nie tworzono cyberwojowników czy cyberżołnierzy od zera. Często wykorzystywano inżynierów, którzy już są, chociażby łącznościowców. W pewien sposób dokonywano ich przekwalifikowania. My też chcemy z tego modelu skorzystać.

Eksperckie Centrum Szkolenia Cyberbezpieczeństwa, które zostało utworzone, ma nam do tego posłużyć. Naszym założeniem było stworzenie jednego centrum kompetencyjnego dla sił zbrojnych. Swego czasu zadawane było pytanie, robili to nawet nasi partnerzy, kto w siłach zbrojnych jest centrum kompetencyjnym w zakresie cyberbezpieczeństwa – i nie było na nie jednoznacznej odpowiedzi. Z jednej strony służby realizowały swoje zadania, z drugiej strony Narodowe Centrum Kryptologii realizowało swoje zadania, z trzeciej strony Centrum Operacji Cybernetycznych również realizowało jakieś zadania. Nie było jasnej, przejrzystej ścieżki wskazującej, z kim należy się kontaktować, nie tylko w kraju, ale również za granicą. Chodziło nam o to, żeby takie centrum kompetencyjne było określone i zdefiniowane.

O maksymalnym wykorzystaniu obecnych zasobów już wspominałem. I o stosowaniu sprawdzonych rozwiązań. Koncepcja przewidywała, że NCBC będzie centrum kompetencyjnym w zakresie cyber, IT i krypto. Ufam, bo pokazał to już ostatni rok, że takowym centrum kompetencyjnym już się stało. Jednocześnie chcielibyśmy zrealizować wszystkie nasze zobowiązania, zarówno wobec NATO, jak i wobec Unii Europejskiej, mówiące o certyfikacji rozwiązań cyberbezpieczeństwa czy reagowania na incydenty komputerowe. Dlatego w ramach NCBC funkcjonuje CSIRT MON, o którym wspominałem, czyli zespół reagowania na incydenty komputerowe. Podstawą do jego funkcjonowania jest ustawa o krajowym systemie cyberbezpieczeństwa.

Etapowe formowanie WOC. Jak wspominałem, cała koncepcja czy cała rotmapa dojścia do osiągnięcia zdolności do działania jest informacją niejawną. Mają państwo do niej dostęp. Przedstawiłem ją w materiałach dodatkowych, które zostały zaadresowane na kancelarię niejawną. Jednak ten wyciąg, którym – jak myślę – mogę się podzielić, mówi o etapowym dochodzeniu. Pierwszy etap już jest za nami. O tym za chwilę powiem. Natomiast jeżeli chodzi o czasowy rozkład, to 2025 r. jest rokiem, w którym będzie pełne dowództwo z pełnym FOK, full operations capability, jeżeli chodzi o cyberprzestrzeń, z certyfikowanym dowództwem i z certyfikowanymi zespołami.

Oczywiście koncepcja uwzględniała i uwzględnia te aspekty, czyli kadry, finanse, formalnoprawne aspekty organizacyjno-strukturalne i współpracę. Widzą państwo, jak swego czasu funkcjonował system reagowania na incydenty komputerowe. Tak to się też nazywało. Był pełnomocnik do spraw bezpieczeństwa cyberprzestrzeni, który odpowiadał za nadzór. Było centrum koordynacyjne w Służbie Kontrwywiadu Wojskowego, centrum wsparcia w NCK i administratorzy w Inspektoracie Informatyki, czyli rozwarstwienie, o którym wspominałem wcześniej. W chwili obecnej, w ramach pierwszego etapu, doprowadziliśmy do zmiany decyzji ministra obrony narodowej i jednoznacznego określenia, kto jest CSIRT-em, gdzie on jest i za co odpowiada.

Określono, że CSIRT MON działa w ramach Narodowego Centrum Bezpieczeństwa Cyberprzestrzeni, jest narodowym punktem kontaktowym pozostałych CSIRT-ów, czyli punktem do współpracy z NATO i z innymi zespołami reagowania na incydenty komputerowe i do współpracy z pozostałymi CSIRT-ami na poziomie krajowym, czyli z CSIRT GOV, który obecnie jest w ABW, i z CSIRT NASK. Określono również, z czego składa się wewnątrz, z jakich zespołów i jakie zadania są realizowane. Ta transformacja rozpoczęła się 20 listopada 2019 r. W ciągu roku już to funkcjonuje w tym składzie, czyli w ramach zobowiązania wynikającego z nowej decyzji. Mieliśmy rok na dostosowanie się do nowej decyzji i do funkcjonowania w ramach tej decyzji, co też zostało uczynione.

Oczywiście ustawa o krajowym systemie cyberbezpieczeństwa zakłada, że to wszystko jest na czas „P”, czyli na czas pokoju. Natomiast na czas „W” minister obrony narodowej jest zobowiązany do przejęcia koordynacji nad obsługą incydentów na poziomie krajowym. Dla nas jest to też i będzie pewnym wyzwaniem, bo musimy nie tylko zbudować kompetencje w ramach naszego CSIRT-u, ale również zapewnić element łącznikowy dla pozostałych zespołów reagowania i zrozumieć ich czasem odmienny tryb pracy przy wyjaśnianiu incydentów.

Stan realizacji koncepcji. Jak wspomniałem, pierwszy etap już jest za nami. Jeżeli chodzi o CSIRT MON, ukompletowanie jest zadeklarowane na poziomie 75%. Zostały opracowane procedury związane z obsługą incydentów komputerowych. Co więcej? Jestem przekonany, że nie tylko monitorujemy nasze systemy, ale też w pewien sposób utwardziliśmy je na tyle – czasem też kosztem funkcjonalności – że odporność systemów resortu obrony narodowej jest już znaczna. To też wpływa na liczbę incydentów. Mają państwo możliwość zapoznania się w materiale dodatkowym z sytuacją. Z tym, jak to wyglądało, jeżeli chodzi o liczbę tych incydentów czy o ich skalę wcześniej. Etap drugi jest przed nami. Oprócz tego, że pozyskujemy kadrę i szkolimy ją, opracowaliśmy doktrynę działań w cyberprzestrzeni. Dalej będziemy pozyskiwać kadry. Będziemy je zgrywać.

Jest jeszcze dość istotne zagadnienie, które – jak myślę – może być nawet przedmiotem kolejnych spotkań u państwa, jeżeli chodzi o Komisję. Jest to aspekt prawny, czyli to, w jakim zakresie żołnierze mogą realizować działania w domenie cyberprzestrzeni.

W chwili obecnej jesteśmy trochę jak pięściarz w ringu – trzymamy gardę i dość dobrze się bronimy. Natomiast nasi partnerzy, chociażby Francuzi i Amerykanie, już dobrze to zdiagnozowali. Amerykanie bardzo dobrze to opisali w swojej strategii z 2018 r., definiując koncepcję pewnych działań w odpowiedzi na działania adwersarzy czy na złośliwe działania przeciwnika, którą nazwali „defending forward". Tam żołnierze nie czekają na wypowiedzenie wojny. Na pewno warto omówić ten temat.

Zleciliśmy też analizę prawną Akademii Sztuki Wojennej. Jest tam pewna ekspertyza, która określa pewne zdolności i możliwości wykorzystania zespołów, które budujemy, jak to jest w bardziej zaawansowanych krajach pod względem działań w cyberprzestrzeni. Mam tu na myśli Stany Zjednoczone i Francję. Te sprawy także u nas należy zdefiniować też na poziomie legislacyjnym, bo tak naprawdę w chwili obecnej budujemy nasze zdolności na czas wojny. Bronimy się w czasie pokoju. Ale jeżeli mówimy o innych typach operacji, to przygotowujemy się do ich prowadzenia. Oczywiście zostaje pytanie, kiedy i w jakim zakresie moglibyśmy z nich skorzystać.

Kolejne działania. Oczywiście to wynika z koncepcji. Formowanie dowództwa też jest pewnym wyzwaniem. Koncepcja utworzenia Wojsk Obrony Cyberprzestrzeni zakładała po każdym etapie możliwość korekty albo możliwość zmiany kolejnego etapu. Wynikało to z możliwości odpowiedzi na obecne zagrożenia. Nie chcieliśmy pisać koncepcji, która będzie obowiązywała przez pięć lat bez możliwości jej zmiany, kiedy zagrożenia zmieniają się co rok, w każdej chwili. To nie miałoby większego sensu. Dlatego założyliśmy, że po każdym etapie będziemy dokonywać rewizji tego, co zrobiliśmy, jak również tego, w którą stronę chcemy iść. W chwili obecnej jest powołany zespół interdyscyplinarny, który określa również dalszy etap – chociażby to, jak ma wyglądać to dowództwo, jak musi wyglądać to dowództwo, żeby w pełni funkcjonowało, ale żeby na tym też nie ucierpiały działania merytoryczne. Bo z jednej strony wojsko przygotowuje się i szkoli, a z drugiej strony nasi eksperci tak naprawdę szkolą się, codziennie broniąc naszych sieci. Tutaj nie mamy takiego etapu, że kończą się ćwiczenia i wracamy do domu, a sprzęt się konserwuje. Tutaj te działania są prowadzone w sposób ciągły. Czasami to trochę przypomina budowanie samolotu w trakcie lotu. Nie jesteśmy w stanie wyłączyć sieci, żeby budować nasze kompetencje. Z jednej strony musimy utrzymywać nasze sieci i monitorować zagrożenia, a z drugiej strony budować nasze kompetencje, co czynimy.

Oprócz naszego zespołu cyberbezpieczeństwa, czyli centralnego zespołu CSIRT w siedzibie NCBC, planujemy również rozbudowę, bo to już zostało uruchomione, kolejnych zespołów cyberbezpieczeństwa, tym razem w regionalnych centrach informatyki, które będą mogły wziąć odpowiedzialność za swoje regiony, żeby utrzymywać je nie tylko pod względem funkcjonalności tych sieci, ale również pod względem ich bezpieczeństwa.

Co więcej? Nie tylko planowanie. Mamy już uruchomiony pewien program budowania laboratorium. To laboratorium już się tworzy. W pewnym zakresie już się ukompletowuje. Natomiast będziemy rozwijać to zaplecze laboratoryjne pod względem testowania sprzętu pod kątem potencjalnych podatności tego sprzętu. Chcemy również certyfikować nasze laboratorium pod względem badań elektromagnetycznych, żeby odciążyć Służbę Kontrwywiadu Wojskowego i Agencję Bezpieczeństwa Wewnętrznego i w tym zakresie, czyli w zakresie tłumienności – fachowo to się nazywa badaniem poziomu zabezpieczenia urządzenia pod względem ulotu elektromagnetycznego – też móc dokonywać testów i analiz na potrzeby sił zbrojnych.

O eksperckim centrum już wspominałem. Oczywiście, to eksperckie centrum rozwijamy. Potencjalne problemy, które pewnie napotkamy na drodze albo możemy napotkać, to chociażby ten aspekt kadrowy. Obecność w cyberprzestrzeni, jak również zagrożenia, które się w niej pojawiają, i ich mnogość powodują, że nawet korporacje czy bardzo dobre firmy mają problemy z zatrudnieniem odpowiedniej klasy specjalistów w swoich szeregach. Z jednej strony to się przekłada na wakaty w domenie cyberprzestrzennej, z drugiej strony wpływa to również na wręcz wykradanie sobie kadr i kłusowanie, czyli oferowanie więcej. I na tym rynku to też się dzieje. W marcu EMIS opublikowała dość ciekawy raport o kadrowych problemach w zakresie bezpieczeństwa cyberprzestrzeni. To bardzo ciekawy raport wskazujący, że w 2019 r. na całym świecie brakowało ponad

4 mln takich specjalistów, co też przekłada się na ich oczekiwania finansowe czy chociażby na ten aspekt, że ciężko jest ich znaleźć.

Jak państwo zauważyli, staramy się sobie radzić na tyle, że jest zainteresowanie pracą i służbą u nas. Zapewniamy też pewną kulturę tej pracy i służby. Kultura pracy żołnierzy służących w NCBC i w przyszłych Wojskach Obrony Cyberprzestrzeni trochę różni się od pracy żołnierzy w jednostkach poziomu taktycznego. Mają niesamowitą możliwość rozwoju. To też pewnie przyciąga do nas. I jeszcze aspekty prawne, o których już wspominałem. To jest teraz zagadnienie, które na pewno będziemy chcieli podnosić nie tylko na poziomie dyskusji, ale również proponowania pewnych rozwiązań legislacyjnych w tym zakresie, bo już zaczynamy dysponować tymi zespołami. Mamy zespoły, które posiadają kompetencje. Warto byłoby rozważyć możliwość wykorzystania tych zasobów czasami również w czasie „P". Ale to będzie wymagało przemyślenia aspektów prawnych.

Musimy działać na podstawie prawa i w ramach obowiązującego prawa, więc na pewno prawo będzie musiało zostać poddane pewnej rewizji, jeżeli chodzi o możliwość wykorzystania żołnierzy w ramach obrony cyberprzestrzeni Rzeczypospolitej Polskiej. Pandemia trochę wpływa na nasze działania, aczkolwiek powiem, że wpływa też pozytywnie pod względem kadrowym. To nie jest tak, że nagle się okazało, że ten rynek jest otwarty na specjalistów, natomiast jeżeli firmy cierpią na braki projektów bądź na niestabilną sytuację w związku z pandemią, to kandydaci czy specjaliści dostrzegają stabilność zatrudnienia w siłach zbrojnych i oczywiście pracy u nas. To się nie zmieniło. Na pewno to też przekuło się na liczbę CV czy na liczbę chętnych. Wielu specjalistów zadeklarowało, że wolą zarabiać mniej, ale mieć zapewnioną stabilność. To też na nas wpływa.

Oczywiście jako organizator wszystkich systemów stacjonarnych w resorcie obrony narodowej w tym okresie nie możemy narzekać na zbyt dużo wolnego czasu. Pracujemy jeszcze bardziej, wręcz ponadnormatywnie, żeby zabezpieczyć funkcjonowanie resortu i sił zbrojnych. Z jednej strony okres pandemii nam pomaga, bo przekłada się na liczbę kandydatów. Ale z drugiej strony oczywiście nie mamy tak bezpośredniego kontaktu i możliwości wyszukiwania jak zwykle. Byliśmy na co dzień obecni chociażby na targach pracy czy w innych miejscach.

Perspektywy pokazuje wyciąg z koncepcji. W 2022 r. nastąpi sformowanie podstawowych struktur dowodzenia dowództwa komponentu. Zaczniemy od uzupełniania obsady. Osiągnięcie częściowej zdolności nastąpi w 2023 r. Następnie będziemy prowadzili proces certyfikacji dowództwa, ale również zespołów, oceniający ich umiejętności. Nie chodzi o to, żeby deklarować, że ma się zespół specjalistów. To nie przekłada się z automatu na to, że oni potrafią działać w cyberprzestrzeni. Nie zawsze każdy zespół, chociażby składający się z indywidualistów, jest w stanie w sposób efektywny realizować działania w cyberprzestrzeni. Chodzi o to, żeby ocenić zgranie tego zespołu i certyfikować ich umiejętności, co koncepcja też zakłada. W 2025 r. nastąpi przeprowadzenie certyfikacji jednostek poziomu taktycznego z minimalną obsadą na poziomie 80% i osiągnięcie pełnej zdolności do prowadzenia pełnego spektrum działań w cyberprzestrzeni.

Plan jest ambitny. Wręcz bardzo ambitny. Ale póki co te półtora roku wskazuje, że idziemy zgodnie z tym planem i efektywnie realizujemy kolejne punkty z naszej mapy drogowej. Oczywiście to nie zakończy się na 2025 r. i na tym, że mamy dowództwo, że to działa. Tak naprawdę przypuszczam, że w 2025 r. już będziemy mówili o innym typie zagrożeń albo o innych domenach operacyjnych, bo to też jest możliwe. Nie wiadomo, jak ten postęp to zmieni i czy cyberprzestrzeń jest ostatnią domeną operacyjną. W moim przekonaniu – nie. Pewnie za 5, 10 czy 15 lat będziemy mówili o kolejnej domenie operacyjnej, o której w chwili obecnej nawet nie jesteśmy w stanie pomyśleć. Tak jak nie myśleliśmy o cyberprzestrzeni 20 lat temu.

Dziękuję bardzo za uwagę. Jeżeli są jakieś pytania, to jestem do państwa dyspozycji.

Przewodniczący poseł Michał Jach (PiS):

Dziękuję, panie generale. Teraz rozpoczniemy cykl pytań. Dziękuję za przedstawienie bogatej informacji. Chcę państwu powiedzieć, że miałem okazję wysłuchać opinii naszych

sojuszników krótko przed pandemią, jeszcze w tym roku w Brukseli, gdy byłem tam w trakcie posiedzenia Zgromadzenia Parlamentarnego NATO. Z przyjemnością słuchałem, że wysoko oceniają sposób działania i tworzenia naszych wojsk. To dobrze o tym świadczy. Przedstawione przez pana generała dane także pokazują, że koncepcja jest właściwie realizowana. Precyzując coś, o czym pan generał już mówił, powiem, że została do państwa wysłana informacja. Warto wiedzieć, że z pełną informacją – tą klauzulowaną, zastrzeżoną – można się zapoznać w sekretariacie Komisji. Bardzo do tego zachęcam.

Bardzo proszę o zabranie głosu pana przewodniczącego Andrzeja Rozenka.

Poseł Andrzej Rozenek (Lewica):

Dziękuję bardzo. Panie przewodniczący, panie ministrze, panie generale, zacznę od pewnej konkluzji, także w nawiązaniu do naszej wizyty w SHAPE na początku tego roku. Nasi sojusznicy z NATO twierdzą, że w zasadzie są tylko trzy europejskie państwa NATO, które w tej chwili są w stanie prowadzić cyberwojnę. Rozumiem, że od tamtego czasu, czyli od początku tego roku, niewiele się zmieniło. Czy pan generał to potwierdza? Byłbym wdzięczny za informację, czy akurat z tymi trzema państwami ściśle współpracujemy, bo takiej informacji nie usłyszałem.

Druga sprawa. Pan generał mówi, że jest zadowolony z postępu prac i z tego, że są dochowane terminy. Rzekomo mapa drogowa jest realizowana właściwie. Natomiast, szanowni państwo, w lutym 2019 r. minister Błaszczak poinformował o powołaniu Wojsk Obrony Cyberprzestrzeni. Minęło półtora roku od tamtej pory. W państwa dokumencie czytam, że już po półtora roku utworzono grupę organizacyjną do spraw sformowania dowództwa Wojsk Obrony Cyberprzestrzeni. Półtora roku zajęło wam sformowanie grupy, która będzie tworzyła dowództwo? To chyba jest tempo niezadowalające.

Mam też prośbę o uszczegółowienie, ponieważ zawsze staram się wyciągnąć z tych wszystkich informacji to, co my możemy zrobić jako parlament dla naszej armii. W punkcie dotyczącym problemów znalazłem chyba coś, co mogłoby być dla nas zadaniem. Piszą tu państwo, że wojska cyberprzestrzeni mogą działać wyłącznie na terytorium Rzeczypospolitej Polskiej. Mogą realizować działania militarne wyłącznie w ramach szkolenia wojsk własnych lub w ramach operacji sojuszniczych – to brzmi bardzo niepokojąco – oraz wyłącznie z zakresu obrony pasywnej. Kiedy przeglądałem zastrzeżenia dotyczące uwarunkowań formalnoprawnych, wygląda na to, że w bardzo szybkim tempie musimy przeprowadzić proces legislacyjny. I moje pytanie jest skierowane chyba bardziej do pana ministra niż do pana generała. Czy resort jest w stanie w miarę szybko przeprowadzić taki proces legislacyjny? Wydaje mi się, że bez wyjaśnienia tych poważnych zastrzeżeń, które tutaj się pojawiły, oraz tych mniej poważnych, jak na przykład pewne uregulowania formalnoprawne, w których chodzi o obowiązek wymagań względem kandydatów i żołnierzy zawodowych, w tym w szczególności stanu zdrowia, sprawności fizycznej, wyglądu itd. Wiemy, że jeżeli mamy do czynienia z ludźmi, którzy zajmują się akurat tą branżą, to może niekoniecznie tężyzna fizyczna jest dla nich najważniejsza. To rzeczywiście też wymaga zmiany. Moje drugie pytanie jest skierowane bardziej do pana ministra. Czy resort jest w stanie przygotować projekt takiej legislacji, który umożliwiłby Wojskom Obrony Cyberprzestrzeni sprawniejsze działanie i lepsze funkcjonowanie? Wydaje mi się, że bez tego ten potencjał po prostu nie zostanie w pełni wykorzystany.

Tak że dwa pytania. Pierwsze o współpracę międzynarodową i o tempo rozwoju Wojsk Obrony Cyberprzestrzeni. A drugie pytanie – do pana ministra – o kwestie legislacyjne. Dziękuję bardzo.

Przewodniczący poseł Michał Jach (PiS):

Dziękuję. Proszę o zabranie głosu pana posła Pawła Poncyljusza.

Poseł Andrzej Rozenek (Lewica):

Karta do czytnika z lewej strony.

Poseł Paweł Poncyljusz (KO):

Tak. Dziękuję bardzo, panie przewodniczący. Panie ministrze, może na początku zacznę od rzeczy organizacyjnych. Jeśli dostajemy informację o tym, że dokument niejawny znajduje się w Kancelarii Tajnej, o godz. 12:42 przed posiedzeniem Komisji, to trudno

jest dać sobie szansę na to, żeby się z nim zapoznać. Bardzo żałuję, że wraz ze spłynięciem dokumentu całkowicie jawnego nie mieliśmy od razu informacji o tym, że rozszerzony dokument jest w Kancelarii Tajnej, bo wtedy mielibyśmy parę dni na przygotowanie się. Nie wiem, czy to była zamierzona intencja, żebyśmy – broń Boże – nie przyszli z tą wiedzą dzisiaj na to posiedzenie i wysłuchali pana generała. Tryb tej pracy jest dość dziwny. Na trzy godziny przed posiedzeniem otrzymujemy informację, że możemy sobie przeczytać ten dokument.

Po drugie, mam taki niedosyt, panie ministrze, bo mieliśmy też rozmawiać o systemie ochrony myśli technologicznej. Taki był temat dzisiejszego posiedzenia Komisji w punkcie pierwszym. Panowie scalili to w jeden punkt, ale w pana wypowiedzi nie zauważyłem – a słuchałem jej, docierając na posiedzenie – żeby coś na ten temat wspomniano. Jest to o tyle istotne, gdyż z tego co wiem, w tej chwili w Ministerstwie Obrony Narodowej, ale chyba też w łonie całej Rady Ministrów, trwają prace nad rozporządzeniem mówiącym m.in. o podstawowym interesie bezpieczeństwa państwa. Na tej podstawie Ministerstwo Obrony Narodowej chce dokonywać decyzji zakupowych, czyli – jak rozumiem – w pewnym sensie wyłączać w jeszcze szerszej skali jakiekolwiek zakupy z przetargów publicznych. Ministerstwo chce używać argumentu o podstawowym interesie bezpieczeństwa państwa, więc rozumiem, że to właśnie wiąże się z systemem ochrony myśli technologicznej.

Rozumiem, że jeśli rozmawiamy o bezpieczeństwie i mówimy o Wojskach Obrony Cyberprzestrzeni, rozmawiamy też o bezpieczeństwie teleinformatycznym. W związku z tym znowu kilka pytań. W jaki sposób szczególnie NCBC interpretuje protokół „secret” w implementowaniu tego na polskie warunki. Z tego co wiem, od wielu lat jest dyskusja o tym, czy to jest „tajne”, czy „zastrzeżone” – i w zależności od tego stawiane są konkretne wymagania różnym rodzajom uzbrojenia. Mówię o pojazdach, ale nie tylko. Chyba ten temat do tej pory nawet w NCK nie był do końca rozstrzygnięty. W armii przez cały czas toczyły się dyskusje o tym, jak to jest. Pokazywano, że w warunkach sprzętu amerykańskiego „secret” to u nas w Polsce niższy szczebel, czyli „zastrzeżone”. Były głosy, że jednak to powinien być wyższy szczebel, co w przypadku pojazdów takich jak Rosomak czy Borsuk jest nie do wykonania. Tak naprawdę to by oznaczało konstruowanie tych pojazdów od nowa, z użyciem innych typów stali, żeby były całkowicie nieprzenikalne, mówiąc kolokwialnie. Chciałbym zapytać, czy ta sprawa jest już jakoś uporządkowana. Czy dalej podlega to interpretacji? To znaczy, że co osoba, co decydent, to inna interpretacja.

Do pana generała mam też pytanie o to, ile osób udało się pozyskać do Wojsk Obrony Cyberprzestrzeni w stosunku do tego, jaki był start. Pan pokazywał tę strukturę przed integracją. Rozumiem, że dzisiaj Wojska Obrony Cyberprzestrzeni w dużej części składają się z tych zasobów, które były w wojsku wcześniej, tylko dzisiaj zostało to inaczej zorganizowane. W związku z tym ile osób przybyło do WOC? Ile z nich przybyło z WOT, a ile spoza armii?

Pan generał mówił o tym, że wojsko staje się atrakcyjne, biorąc pod uwagę, że wielu informatyków staje przed dylematem, czy mają gdzie pracować, czy nie. W dobie COVID-u te firmy też często zwalniają. Jest pytanie, jak to jest na dzień dzisiejszy?

Następne pytanie, panie generale. Być może jest to pytanie do pana ministra, aczkolwiek sądzę, że to właśnie pan będzie to wiedział. Jak pan zapatruje się na problem tzw. radiostacji IP, które nie mogą być wyłączone? Nie mogą być w całkowitej ciszy radiowej. Taki przypadek mieliśmy na Ukrainie w czasie wojny, kiedy Ukraińcy zakupili amerykańskie radiostacje pokładowe i zamontowali je w pojazdach. Był fetysz radiostacji IP, po czym okazało się, że nie istnieje tam możliwość całkowitej ciszy elektronicznej tych radiostacji. Skończyło się na tym, że Ukraińcy usunęli te dość nowoczesne radiostacje z pojazdów i założyli ponownie stare rosyjskie analogowe radiostacje. Na ile ten fetysz IP przy radiostacjach na szczeblu taktycznym, czy to pokładowych, czy to plecakowych, czy doręcznych, pana zdaniem da się rozwiązać? I czy da się go rozwiązać polskimi siłami?

Mówię o tym właśnie w związku z walką elektroniczną, która po stronie rosyjskiej jest bardzo dobrze rozbudowana i to na wielu szczeblach. Z jednej strony jest to identyfikowanie konkretnych celów przeciwnika – czy to będą pojazdy, czy to będą nawet

pojedynczy żołnierze posiadający właśnie sprzęt, który sieje, mówiąc kolokwialnie. Z drugiej strony jest to również to, z czym mamy do czynienia na Ukrainie, czyli odcinanie górnej półkuli, w związku z czym obiekty latające nie mogą być obsługiwane przez żadne nadajniki, czy to satelitarne, czy to naziemne, na przykład przez trackery. To było widać na Ukrainie. A w tej chwili w konflikcie Armenii w Górskim Karabachu również to się pojawia.

Chciałbym mieć też pytanie do pana ministra. Jak się miewa program „Tytan", jeśli chodzi o nową radiostację taktyczną? To jest historia chyba z ośmiu lat. A biorąc pod uwagę właśnie nowe wyzwania związane z cyberbezpieczeństwem, z walką elektroniczną, to wszystko ma kolosalne znacznie, zważywszy na to, że radiostacje, którymi dzisiaj dysponuje wojsko, mają już swoje lata. Jaki jest stan państwowych badań tych radiostacji? Kiedy planują państwo ich wdrożenie do sił zbrojnych? Niewątpliwie takie urządzenia są potrzebne, chyba że założenie jest takie, że kupimy je za granicą i w ten sposób rozwiążemy problem. Aczkolwiek w związku z tym na pewno polski przemysł nie pójdzie do przodu ani gospodarczo, ani technologicznie.

Chciałem się również dowiedzieć, jak panowie się zapatrują w ramach bezpieczeństwa teleinformatycznego na kwestię łączności, która dzisiaj jest zamontowana w takich pojazdach, jak T-72, PT-91 i czołgi Leopard. Z tego co mi wiadomo, są tam radiostacje analogowe, które dość prosto można zagłuszyć. To oznacza, że bezpieczeństwo teleinformatyczne, bezpieczeństwo łączności jest zdane na wyposażenie przeciwnika w odpowiedni sprzęt. Jeśli nie ma odpowiednich zagłuszarek, jest szansa, że załogi poszczególnych pojazdów będą miały kontakt między sobą czy ze swoimi przełożonymi. A w momencie, kiedy takie zagłuszarki będą dostępne po stronie przeciwnika, praktycznie kończy się cała łączność.

I ostatnia rzecz. Od dawna pojawia się dyskusja odnośnie do tego, w jakim protokole powinny być szyfrowane radiostacje, szczególnie szczebla taktycznego czy to doręczne, czy pokładowe w pojazdach. Z jednej strony jest grupa zwolenników protokołu SCIP. Jest też grupa zwolenników protokołu AES, czy to w kluczu 256 bitów, czy nawet niższym. Z tego co wiem, może być nawet wyższy klucz. Jak pan generał zapatruje się na te dwa protokoły? Bo wygląda na to, że cały czas jest taka wojna postu z karnawałem w strukturach wojska, jeżeli dobrze rozumiem, odnośnie do tych dwóch różnych protokołów, trochę się wykluczających. Biorąc pod uwagę to, że AES jest cały czas rozwijany i staje się popularny do tego stopnia, że jakąś wersję…

Przewodniczący poseł Michał Jach (PiS):

Dziękuję, panie pośle. Minęło dziesięć minut. Dziękuję.

Poseł Paweł Poncyljusz (KO):

Czyli będę jeszcze raz prosił o głos. Dobrze. Poproszę jeszcze raz o głos.

Przewodniczący poseł Michał Jach (PiS):

Bardzo proszę. Czy jeszcze ktoś chce zabrać głos? Pani poseł. Bardzo proszę. Pani poseł Monika Pawłowska.

Poseł Monika Pawłowska (Lewica):

Szanowny panie przewodniczący, szanowny panie ministrze, panie generale, Wysoka Komisjo, w informacji o Wojskach Obrony Cyberprzestrzeni jest bardzo dużo informacji cennych, ale brakuje najważniejszej, czyli informacji o pieniądzach. Skąd? Za ile? Za co? Bo zagrożenie ze strony Rosji istnieje nie od dzisiaj. Jak wspominał przewodniczący Rozenek, te wojska były zapowiadane już wcześniej. Średnio się to spina z wcześniejszym kalendarzem. Chciałabym zapytać, ile chcą państwo przeznaczyć w budżecie na cyberbezpieczeństwo?

Nie chciałabym o tym mówić, ale teraz po prostu brakuje pieniędzy na wszystko. Były tworzone Wojska Obrony Terytorialnej, które też miały być o wiele większe. Na ostatnim posiedzeniu Komisji dowiedzieliśmy się, że jednak i na to brakuje pieniędzy, pomimo tego, że budżet Wojsk Obrony Terytorialnej jest taki jak budżety wywiadu i kontrwywiadu. Tak są dotowane. Stąd moje pytanie. Mówimy o wojskach, o obronie, o tym, że zawodowi wojskowi nie są za bardzo dotowani. Nie mają nawet mundurów, broni

etc. Działań w zakresie cyberbezpieczeństwa nie da się realizować na starych laptopach, więc pytanie – skąd i za co? Z informacji, których nam pan udzielił i które były zapisane, wynika, że przewidują państwo, że problemem może być brak specjalistów o wymaganych kwalifikacjach i brak konkurencyjności w wymaganiach dla specjalistów.

Czy ministerstwo ma więcej informacji o tym, jak wygląda obecna sytuacja na rynku IT w Polsce i w Unii Europejskiej? Ile zarabiają najlepsi specjaliści z zakresu cyberbezpieczeństwa? Czy ministerstwo posiada wstępne informacje o tym, ilu studentów będzie zainteresowanych właśnie tą jednostką w zakresie obronności? W porządku, mamy studentów – ale czy oni będą zainteresowani służbą po ukończeniu studiów? Dziękuję serdecznie.

Przewodniczący poseł Michał Jach (PiS):

Dziękuję. Bardzo proszę, panie ministrze i panie generale o udzielenie odpowiedzi.

Sekretarz stanu w MON Wojciech Skurkiewicz:

Myślę, że w zdecydowanej większości odpowiedzi udzieli pan generał. Ja tylko, jeżeli chodzi o panią poseł. Jest tak, że jeżeli ktoś decyduje się na to, żeby podjąć studia na kierunku wojskowym w wojskowej uczelni, to jest podchorążym. Jest już żołnierzem, więc ma również świadomość tego, jakie będą na nim spoczywały obowiązki w momencie, kiedy otrzyma promocję oficerską i zostanie skierowany do służby zawodowej. Jest tak, że oni mają pełną świadomość. I jest to jeden z elementów.

Dziś, jak powiedziano, wiodącą uczelnią jest Wojskowa Akademia Techniczna, jeżeli chodzi o kształcenie podchorążych w obszarze cyberbezpieczeństwa, ale również – szeroko rzecz ujmując – w obszarze IT. Chcemy stworzyć taki system, żeby również w pozostałych uczelniach wojskowych, także w tym obszarze – chociaż może nie w takiej skali jak na Wojskowej Akademii Technicznej – kształcić podchorążych. Dlatego rozwijamy ten obszar. On się fajnie rozwija na Akademii Marynarki Wojennej. Uruchamiamy również na akademii we Wrocławiu kierunek informatyczny. Tak, żebyśmy mieli jak najszerszy front studentów podchorążych, którzy będą mogli zasilać ten obszar. Oczywiście bardo szeroko posiłkujemy się również cywilnymi ekspertami, czyli pracownikami, którzy chcą się z nami związać w formule pracownika resortu obrony narodowej albo zasilić nasze szeregi jako żołnierze Wojska Polskiego. Dlatego, jak wspomniał pan generał, są określone zachęty. Próbujemy pozyskiwać specjalistów z rynku cywilnego.

Zdajemy sobie sprawę, że w wielu aspektach nie jesteśmy w stanie sprostać oczekiwaniom finansowym. Mamy tego świadomość. Dlatego zachęcamy w formie dodatkowych środków finansowych, które dyrektor NCBC ma w ręku. Ma określone instrumenty, które może stosować poprzez dodatkowe bonusy czy dodatkowe wynagrodzenie tych osób czy żołnierzy. Jeżeli chodzi o samą formułę kształcenia, to nieprzypadkowo w 2019 r. podjęliśmy decyzję o tym, żeby ten system był spójny i żeby kształcić młodych ludzi praktycznie od poziomu szkoły ponadpodstawowej czy ponadgimnazjalnej. Przypomnę, że w 2019 r. rozpoczęliśmy nabór do Wojskowego Ogólnokształcącego Liceum Informatycznego przy Wojskowej Akademii Technicznej. Przyznajemy, że liczba osób, które się zgłosiły w pierwszym roku, przeszła nasze najśmielsze oczekiwania. W momencie startu tego liceum liczba kandydatów przekroczyła 10 osób na jedno miejsce. Otworzyliśmy dwie klasy. Klasę po gimnazjum i klasę po szkole podstawowej.

W tym roku będą kolejne dwie klasy, więc mamy setkę młodych ludzi, którzy naprawdę są olbrzymim – powiedziałbym, że wręcz gigantycznym – potencjałem dla nas jako sił zbrojnych, ale również dla Wojskowej Akademii Technicznej. Jestem przekonany, że zdecydowana większość – jeśli nie niemal wszyscy – zasili szeregi Wojskowej Akademii Technicznej, a w przyszłości być może również szeregi naszej armii. Śledzę doświadczenia liceum lotniczego w Dęblinie. Absolwenci tego liceum – tak bliskiego pani poseł – niemal w 100% zasilają lotniczą akademię, więc liczę, że tutaj będzie bardzo podobnie.

Jeżeli chodzi o budżet tego obszaru, jest on realizowany na takim poziomie, jakie są oczekiwania tworzących tę strukturę. Mam tutaj na myśli pana generała Molendę. To jest obszar, w którym zmienia się technika czy trendy – nie powiem, że nie ma tu możliwości oszczędzania, ale jest to obszar, który musi być również doceniany finansowo

w związku ze zmieniającą się technologią, w której operujemy. Myślę, że więcej na ten temat powie pan generał.

Dyrektor NCBC gen. Karol Molenda:

Zacznę od początku, od pytań pana posła. Trzy państwa potrafią czy są w stanie prowadzić cyberwojnę. W ogóle musielibyśmy zacząć od tego, co to jest cyberwojna. Ale tutaj wchodzilibyśmy w jakiś wykład akademicki. Myślę, że to nie o to chodzi. Chodzi o to, czy zespoły, którymi dany kraj dysponuje, są w stanie prowadzić operacje w cyberprzestrzeni w pełnym spektrum. Operacje w cyberprzestrzeni dzielą się na operacje obronne i ISL czyli intelligence, surveillance and reconnaissance, a inaczej – rozpoznanie i działania ofensywne. To jest zestaw trzech rodzajów działań zdefiniowanych przez NATO. Faktycznie w ten sposób można oceniać zdolności pewnych krajów.

Nie tyle trzy, ile nawet piętnaście krajów określiło, że posiadają pełne zdolności. NATO jako struktura obronna zadeklarowało, że nie buduje zdolności ofensywnych. W razie potrzeby będzie wykorzystywało zadeklarowane przez inne kraje zdolności ofensywne. Faktycznie wiele krajów takie zdolności zadeklarowało. Odmienną kwestią jest to, czy je posiadają. Co jest specyficznego w tych operacjach cyberbroni? Tak możemy to nazwać. Czym ona się różni od innych? To jest dość ciekawe, bo z jednej strony dla tej cyberbroni, dla jej wytworzenia, trzeba zrobić bardzo dużo inwestycji. Nie tylko intelektualnych, ale również dla przykładu znaleźć podatność. Znaleźć tzw. podatność zero-day, o której nikt nie wie, żeby ona była stuprocentowa, i stworzyć kod, czyli malware, który może ją wykorzystać. Często może ją wykorzystać tylko raz. I ona już nie jest do użycia. Jeżeli raz się ją wykorzysta, druga strona to zauważy. Co więcej, są jeszcze pewne zabawy związane z tym, że tę broń można wykorzystać przeciwko jej autorowi, czego przykłady już mieliśmy w historii. Chociażby Amerykanie, którzy wykorzystywali zdolności ofensywne, później nie zawsze byli gotowi, żeby sami się zabezpieczyć przed swoimi kodami. Jeśli coś jest podatnością zero-day, to znaczy, że na to nie ma łaty bezpieczeństwa.

Ale mówimy o współpracy. Tak, jeżeli chodzi o współpracę z partnerami. Tu nawet nie chodzi o podpisanie porozumienia. W ciągu półtora roku mogliśmy podpisać 15 czy 20 porozumień. Powiedzmy sobie, że znam takie jednostki – bez różnych nazw – które taką liczbę porozumień podpisały. Jest pytanie, czy to porozumienie żyje. Jeżeli po drugiej stronie ktoś zadzwoni i powie, że coś się dzieje, to czy ktoś mu odpowie, bo jest dla niego partnerem? Tu chodzi o budowanie relacji. I to jest trudniejsze zadanie. Żeby zbudować relacje z takimi graczami – jak powiedział pan poseł – którzy inwestowali w swoje zdolności przez lata, trzeba powiedzieć, że jestem dla was partnerem. Oni nie otwierają drzwi dla każdego, kto mówi, że buduje takie wojsko. Nie mówią: OK, budujecie wojska, to chodźcie. To my w pewien sposób swoimi zdolnościami udowadniamy, że jesteśmy partnerem do dyskusji. Że możemy coś wspólnie zrobić. Że mamy wiedzę. Co więcej, z powodu tego, gdzie jesteśmy geograficznie, niektórzy przeciwnicy na naszych systemach testują swoje zdolności, zanim pójdą dalej, więc jest pewna współpraca.

Co więcej mogę powiedzieć? Po półtora roku ufam, że wśród części tych graczy z czołówki, o których pan poseł mówił, wspominał, jesteśmy już zauważani jako potencjalny partner. Ale to też są tematy różnych relacji w danym kraju, różnych relacji wynikających nie tylko z tego, ale że na przykład współpracujemy z innymi krajami, a komuś może nie jest z tym po drodze – to są na pewno takie pewne niuanse. Bardzo zależy mi na tym, żeby kiedy będzie ta współpraca – a taką mogę zadeklarować i myślę, że strona amerykańska może też o tym powiedzieć – móc powiedzieć, że współpraca z jednym z tych partnerów jest wręcz na poziomie taktycznym. Że jest współpraca, w której zespoły mają swobodę komunikacji między sobą oraz wymianę informacji i swoich umiejętności. Oczywiście są jeszcze partnerzy, nad którymi pracujemy.

Odnosząc się do tego, muszę bronić swoich racji. W dniu 5 lutego 2019 r. zostałem powołany jako pełnomocnik ministra do spraw utworzenia Wojsk Obrony Cyberprzestrzeni. Nie utworzono WOC, tylko pan minister zadeklarował, że takie wojska utworzy. Co więcej, na mocy decyzji nr 17/19, która określiła mnie jako pełnomocnika, miałem do końca czerwca opracować koncepcję. Nie było tak, że usiadłem i zacząłem pisać kon-

cepcję, bo po prostu należało przejrzeć to, co mamy w siłach zbrojnych. Także z racji tego, że przez 12 lat byłem jakby trochę z boku sił zbrojnych, biorąc to zawodowo. Bardziej zajmowałem się bezpieczeństwem, czyli cyberkontrwywiadem, więc najpierw musiałem poczuć, co jest, żeby tę koncepcję stworzyć. Ta koncepcja została stworzona. Została zatwierdzona 12 września, bo oczywiście podlegała też analizom w resorcie obrony narodowej.

Nie było tak, że Molenda napisał sobie koncepcję, a minister ją zatwierdził. Musiała przejść przez ścieżkę zdrowia, jak to nazywam. Jeżeli ktoś uzgadniał coś w jakimś resorcie, może sobie odpowiedzieć, jak to było łatwe. Ale się udało. Co do dowództwa, jak wspominałem, koncepcja zakładała pewien harmonogram. W 2022 r. zaplanowano powołanie dowództwa. To nie znaczyło, że już musimy powoływać grupę do jego utworzenia, bo widzieliśmy w harmonogramie, że w 2022 r. będzie miejsce na tymczasowe dowództwo, a w 2024 r. na dowództwo docelowe. Ta grupa do spraw dowództwa nie powie mi, jakie to ma być dowództwo. Robimy różne ćwiczenia i gry, więc to wiemy. Natomiast jest to tylko taka część administracyjna. Każdemu trzeba opracować zakres obowiązków. Trzeba wykonać ten nalot administracyjny, który się z tym wiąże, z tymi procedurami. Ktoś to musi wykonać. Ja fizycznie nigdy tego nie robię, więc musi to robić grupa.

Dlatego w ubiegłym roku skupiliśmy się na pierwszym etapie, czyli na obronie naszych sieci, na zbudowaniu CSIRT MON, na pozyskiwaniu ludzi do CSIRT MON. Stwierdziliśmy, że najważniejsza jest dla nas teraz obrona tej sieci. Nie będzie tak, że będziemy tworzyć dowództwo, a tu będą nam wyciekać dane. Przyjęliśmy, że najpierw bronimy, a później tworzymy dowództwo itd. To jest jeden z wzorów, którym poszliśmy. Są kraje, które poszły całkowicie inaczej. Są takie, które powiedziały, że od dzisiaj mamy dowództwo i to znaczy, że mamy wojsko. Powiem tak. Nie będę wymieniał publicznie, które to kraje. Powiedzmy sobie, że kiedy rozmawia się z dowódcami tych cybercommand, nie czują się komfortowo z tym, że mają dowództwo. Fajnie, że są wodzowie. Ale kiedy nie ma Indian, to nie ma za bardzo kim dowodzić.

Dlatego my wyszliśmy z tego inaczej. Najpierw zespoły. Najpierw budujemy kompetencje. A kiedy będzie już kilka zespołów i będzie można koordynować prace między zespołami, współpracę itd., wtedy dowództwo nam się przyda. Ale od tego nie zaczynajmy. A mogliśmy pójść drogą PR i powiedzieć, że mamy dowództwo i mamy armię. Byłem przeciwnikiem tego. I cieszę się, że pan minister zaakceptował tę wizję, że dowództwo jest jednym z ostatnich etapów, że najpierw szukamy Indian, a później wodzów, bo jak są sami wodzowie, to różnie jest z pracą. Oczywiście jest nabór. To, że prowadzimy nabór ludzi, to jedno. Natomiast jest cały background check, czyli poświadczenia bezpieczeństwa. Są całe procedury związane z uzyskaniem poświadczeń bezpieczeństwa dla tych żołnierzy do spraw tajnych czy ściśle tajnych. To są czasochłonne procedury, które też wpływają na nasze zasoby

W odpowiedzi dla pana posła Poncyljusza też nawiążę do tego pytania. To się dzieje. O tym wspominała pani poseł. Tak, wiemy. Mam pełną analizę. Co więcej, mam wielu kolegów, którzy gdzieś działają. Dobrze wiem, ile zarabiałbym na rynku, Natomiast nie jest aż tak. Jeżeli ktoś na dzień dobry deklaruje, że finanse są dla niego ważniejsze niż… Finanse są ważne. Ale kultura pracy i wyzwania, to jest coś, co na przykład przyciąga – jak zauważyłem – moich współpracowników do zespołu. Kultura i wyzwania. Oni spotkają się tu z zadaniami, z którymi nie spotkają się nigdzie indziej. Być może gdzieś w bankach, ale to jest całkowicie inny target.

Dla przykładu powiem, że kiedy mówimy o cyberprzestępcy, to mówimy o kimś, kto chce uzyskać korzyści majątkowe, chce wyciągnąć to od użytkownika cyberprzestrzeni. Co robi ten cyberprzestępca? On zazwyczaj sięga po najniżej wiszący owoc. Jeżeli system pani poseł będzie trochę lepiej zabezpieczony niż sąsiadki pani poseł, to po zrobieniu testów przestępca pójdzie tam. Po co ma tracić siły i energię, przełamywać zabezpieczenia, kiedy może skorzystać z tego i osiągnąć cel. Wyciągnąć numery kart kredytowych, pieniądze itd. od kogoś, kto jest nieświadomy bezpieczeństwa i tych zagrożeń.

To są cyberprzestępcy. A my mówimy o całkowicie innych aktorach. U nas mówimy często o aktorach, którzy są strukturami sformalizowanymi, które dostają polecenie, żeby iść wyciągnąć dane z określonego miejsca. Często hakerzy, którzy działają pod egidą

obcych służb, dostają polecenia. Oni nie przyjdą do swojego mocodawcy i nie powiedzą: tu było za ciężko, ale wyciągnąłem coś z innego ministerstwa, co może się przyda. No nie. Bo on dostał konkretne zadanie. Jeśli dzisiaj mu się nie uda, spróbuje jutro, pojutrze itd. Będzie próbował do skutku, bo ma do tego motywację, ma do tego umiejętności i ma też takie polecenie. My spotykamy się z takimi przeciwnikami po drugiej stronie. I musimy im sprostać, co też niesamowicie buduje zespół. Zauważyłem, że to bardzo pozytywnie wpływa na zespół, który jest po drugiej stronie, czyli jest u nas. Bo to jest po prostu tak, że dzisiaj byłem lepszy niż tamten. Nie jest tak, że dzisiaj była kampania, a jutro jej nie ma, bo zazwyczaj jutro też jest. Często nie prowadzi się działań w weekendy. Zauważyłem taką prawidłowość. Kiedyś było tak, że w weekendy było częściej. A teraz widzę, że ci, którzy nas atakują, pracują 8 godzin, w tygodniu od poniedziałku do piątku. W godzinach w pewnej bliskiej nam strefie czasowej.

Oczywiście to jest temat atrybucji. Możemy tutaj mówić: kto, co, jak itd. Temat atrybucji i ataku jest tematem złożonym i do tego bardzo ciężkim. Natomiast są pewne niuanse, które pewnie na jakiejś innej – niejawnej, zamkniętej sieci mogę państwu przedstawić, wskazujące na konkretnych aktorów, jeżeli chodzi o obronę.

Co do działań wojsk cyberprzestrzeni, jest to temat o tyle złożony, że to nie tylko nasze ustawodawstwo, ale ogólnie ustawodawstwo ONZ i międzynarodowe określa pewne zasady. Może podam pewien przykład. Jeżeli jest atak, to teoretycznie odpowiedzenie siłą powinno się odbyć po wyczerpaniu wszystkich możliwych mechanizmów. Czyli powinniśmy wykorzystać naszą dyplomację. Pewnie powinniśmy napisać notę, że sobie tego nie życzymy, przy założeniu, że wiemy, kto to zrobił. I teraz wykorzystanie armii. Możemy tu wskazać kraj, może bez podawania nazwy, który jest w stanie wojny. To jest trochę inaczej, jeżeli chodzi o wykorzystanie tych żołnierzy, bo oni są w stanie wojny. I teraz przykład jednego z incydentów. Nasz przeciwnik atakował nas z infrastruktury cywilnej. Ze szpitala. Czyli używał komputerów w szpitalu, żeby nas zaatakować. I teraz – jak pan poseł pytał – czy wojsko może odpowiedzieć do infrastruktury cywilnej innego kraju? To są tak złożone procesy. Jestem chętny do dyskusji z państwem, tylko może przygotuję się z tego z moimi specjalistami. To naprawdę nie jest czarno-białe. Było *50 twarzy Greya*, a to jest 50 odcieni szarości. To nie są wartości binarne. Jeżeli armia będzie wykorzystana do tego, żeby zaatakować infrastrukturę cywilną innego kraju, to już naprawdę gdzieś musi paść komenda. Natomiast jest też taki fakt, że Francuzi i Amerykanie przepracowali to u siebie. Mają już zdefiniowane, jak kraj na poziomie politycznym odpowie, jak będzie traktował atak na swoją infrastrukturę. I jak najbardziej jest tu miejsce do naszej dyskusji i dla państwa jako ustawodawcy do określenia pewnych warunków, żebym wiedział, że mogę wydać jakieś polecenie i że po prostu nie przekraczam swoich zdolności. Panie przewodniczący, jeżeli moglibyśmy zaplanować jakieś następne spotkania na ten temat, to jak najbardziej tak. Przygotuję się ze swoim zespołem, bo dla mnie to jest kluczowe. Kiedyś, gdy tych zespołów nie było, skupiałem się na obronie. Teraz, kiedy już są, być może warto byłoby pomyśleć o czymś więcej.

Dobrze. Odpowiem na pytania pana posła Poncyljusza. Może zacznę od cyber. Wojska Obrony Terytorialnej tworzą swój komponent w ramach WOT, czyli zespoły działań cyberprzestrzennych. Jest to stuosobowy zespół. Zostało to zadeklarowane na razie w dowództwie. Natomiast to nie są osoby, które my pozyskujemy. To jest całkowicie inny typ osób. To jest specjalista, który funkcjonuje na rynku cywilnym. Jest mu tam dobrze i on nie chce przyjść do nas, żeby pracować od poniedziałku do piątku w określonych godzinach. Ma dobrą pracę, ale na przykład w weekendy jak najbardziej może nas wspierać. To jest całkowicie inny typ.

Trochę na wzór amerykański otworzyliśmy się na tych, którzy mają dobrą pracę i nie chcą jej zmieniać. Realizują się tam, ale mogą coś zrobić dla ojczyzny albo założyć mundur i być może pobiegać po poligonie. Nie wiem, co nimi głównie kieruje. Być może to, o czym zawsze wspominam, że realizowanie działań z flagą na ramieniu dla wielu jest też pewną wartością samą w sobie. Czyli WOT jest WOT-em. Oni jak najbardziej budują swoje zespoły. Te zespoły będą teraz szkolone. Ich umiejętności będą doskonalone i będą zgrywane, o czym wspominałem, w ramach Eksperckiego Centrum Szkolenia Cyberbezpieczeństwa. Tam te zespoły będą szkolone. Oczywiście w ramach potrzeb one trafią

pod moje dowodzenie czy pod dowodzenie kogoś, kto będzie dowodził tymi wojskami w przyszłości. Tak to jest. Jeżeli chodzi te zespoły, które my zbieramy, to są w nich osoby, które chcą założyć mundur i z nami służyć, bądź pracownicy cywilni, którzy będą z nami pracowali.

W informacji niejawnej nigdy nie podawaliśmy liczby ludzi. Koncepcja także nie zakładała liczby ludzi. Natomiast powiem, że w tym roku w centrum i w przyszłych Wojskach Obrony Cyberprzestrzeni zatrudniliśmy kilkaset osób. O ile dobrze pamiętam, w materiale niejawnym mają to państwo rozliczone dokładne, nawet w tabelce, jeżeli chodzi o te osoby, które przyszły. W chwili obecnej, to jest w tym miesiącu, mam rozpoczęte sprawy 73 cywili i 52 żołnierzy zawodowych. Co miesiąc to napływa. Te procesy są realizowane. Nie chciałbym podawać skali. Ale nie przyjmujemy z Wojsk Obrony Terytorialnej. Może inaczej, bo mogę coś przekłamać. Jeżeli w Wojskach Obrony Terytorialnej był jakiś żołnierz zawodowy, to być może któryś mógł do mnie trafić. Ale nie było tak, że przyszło ich 10 czy 20. Mogło być tak, że jeden czy dwóch oficerów przeszło do nas w ramach kłusowania wewnątrz struktury.

Bo pozyskujemy młodych oficerów, oficerów młodszych. Ale liderów też gdzieś muszę szukać. Muszę ich pozyskiwać po prostu z sił zbrojnych – starszych oficerów. Często są to łącznościowcy, których przekwalifikowujemy. Starszych oficerów nie wygenerujemy. A chyba tym bardziej nie chcielibyśmy z podporucznika robić pułkownika w krótkim czasie. Na lidera, na dowódcę zespołu, szefa oddziału, szefa szefostwa ktoś musi zapracować. Być może faktycznie zdarzają się pojedyncze osoby, które będąc żołnierzami zawodowymi, trafiły do nas ze struktur Wojsk Obrony Terytorialnej. Natomiast jeżeli mówimy o terytorialsach, to nie, takiego przypadku nie było.

Jeżeli chodzi o te protokoły, to też jestem otwarty na dyskusję na ten temat. Też mogę się do tego przygotować. Natomiast „secret" to „secret". „Secret" rozumiemy jako „tajne". Tutaj nie ma wątpliwości. W ramach porozumienia pomiędzy USA a Polską „secret" to „tajne". Tutaj nie ma żadnej nadinterpretacji. Nie możemy o tym mówić. Możemy mówić o tym, że Amerykanie nie mają „restricted". Tak możemy mówić. Ale „secret" jest „secret". I „secret" jest „tajne". Jeżeli chodzi o nas jako o centrum, to zajmujemy się kolejną domeną, o której dzisiaj nie wspominałem, czyli kryptografią i opracowywaniem algorytmów. Mamy również kilka rozpoczętych projektów, jeżeli chodzi o szyfratory.

Pan poseł wspominał o SCIP, NAIM i AES. I w jednym, i w drugim są prowadzone prace. Dostajemy zapotrzebowanie sił zbrojnych. Ja nie narzucam. Nie mówię, że komuś przydałby się taki czy taki szyfrator. Jako odbiorca tematu dostaję zapotrzebowanie od gestora. Niestety nie czuję się upoważniony do odpowiedzi na część pytań pana posła, bo to nie ja jestem gestorem systemów wsparcia dowodzenia. Ja odpowiadam za systemy stacjonarne w siłach zbrojnych. Czyli za sieci teleinformatyczne. Jeżeli chodzi o systemy radiowe wsparcia dowodzenia, póki co – nie. Chyba że są jakieś plany co do mojej osoby. Tu jest gestor, akurat w Dowództwie Generalnym. Nie chciałbym mu odbierać chleba. Natomiast z inżynierskiego punktu widzenia – myślę, że mogę o tym powiedzieć – ja to tak rozpatruję i przypuszczam, że wszyscy gestorzy rozpatrują to podobnie.

Takie działania jak na Ukrainie, czyli takie konflikty, które są w tej chwili na świecie, są fantastycznym poligonem, żeby uzyskać know-how, czyli wiedzę, co się sprawdziło, a co się nie sprawdziło. Ja przynajmniej tak robię. I odpytuję różne instytucje, które są w stanie zasilić mnie wiedzą związaną też z rozpoznaniem w tym zakresie. Nasze inwestycje, o czym wspominała pani poseł, jeżeli chodzi o plany i finansowanie, wynikają z tego, że w armii określa się pewne zdolności, które armia musi pozyskać. To się przekłada na program operacyjny. A tam jest na to odpowiednie finansowanie. Nasze badania, rozwój, plany i zdolności wynikają nie tylko z naszej wiedzy, że nam się wydaje, że może to tak zrobić, tylko także z tego, co teraz dzieje się na świecie. Jeżeli materializują się pewne zagrożenia, to jakimi narzędziami musimy dysponować, żeby przeciwstawić się tym zagrożeniom.

Ale też, jak podąża świat. Jakiś czas temu części tych urządzeń nie było. Teraz mówimy o innych typach sprzętu, który pojawia się na co dzień chociażby w naszych domach. W przyszłości pewnie nie tylko dla nas będzie to stanowiło nie tylko wartość dodaną, ale

też niesamowite zagrożenie. Powiedzmy sobie szczerze, jeżeli coś kosztuje kilkaset dolarów, to jakie mechanizmy bezpieczeństwa są tam zaimplementowane. Mówimy raczej o głupich urządzeniach, a nie o urządzeniach inteligentnych. Wbrew pozorom w przyszłości trzeba o tym pomyśleć, bo to może być dobry przykład na wykorzystanie ataku. Bywały już takie ataki. Nie chciałbym skłamać, ale kilkaset tysięcy kamerek internetowych zaatakowało komputery. Ktoś przejął kamerki na świecie i atakował nimi systemy teleinformatyczne.

Teraz pomyślmy. Kiedy myślimy o bezpieczeństwie cyberprzestrzeni naszego kraju, w naszych analizach są też badania, opracowanie pewnych badań czy zdolności, żeby uwzględniać te zagrożenia, które może nie są mocno obecne w tym roku, ale za pięć lat prawdopodobnie będą. Stąd wspominałem o nowej domenie, która kiedyś powstanie. Jestem przekonany, że cyberprzestrzeń nie jest ostatnią domeną, z którą przyszło się nam borykać. Pojawią się nowe. Być może pojawią się domeny związane z innymi działaniami albo ze strefą informacyjną, która dość mocno teraz się rozwija. Można się zamknąć jak gdyby w bańce mydlanej związanej ze swoimi mediami społecznościowymi, w której pewne algorytmy związane z uczeniem maszynowym czy pewną sztuczną inteligencją będą wpływały na nasze widzenie świata. Jeśli nie mamy tej świadomości, możemy tkwić w tej bańce mydlanej. To, jeżeli chodziłoby o te sprawy.

Co mówimy, myśląc o szyfratorach. Głównie skupiamy się na NAIM i SCIP. Dlatego że są to protokoły, które są rozwijane w ramach NATO, a bardzo nam zależy, żeby nasze urządzenia były interoperacyjne z urządzeniami naszych sojuszników. Musimy mieć szyfratory. Opracowujemy je. Jestem przekonany, że nam się uda. Nawet już chyba mogę się jednym pochwalić, który został opracowany przez NCBC i jest wdrażany. To nasze szyfratory, które wykorzystują technologię SCIP i NAIM. A z drugiej strony zapewniają pewną interoperacyjność z naszymi partnerami. Czyli jest możliwość federowania sieci w ramach wspólnych operacji. To chyba do tego się dąży.

Przepraszam pana posła Poncyljusza, ale nie czuję się upoważniony, żeby odpowiedzieć na część pytań. To nie jest w zakresie działania narodowego centrum. To jest dowództwo. Jeżeli te pytania będą podtrzymywane, to ewentualnie mogę je przekazać do właściwego gestora, któremu nie chciałbym odbierać chleba. Tym bardziej że mógłbym jeszcze wprowadzić w błąd, więc nie chciałbym tego robić. Z mojej strony to wszystko. Dziękuję.

Przewodniczący poseł Michał Jach (PiS):

Dziękuję.

Poseł Janusz Korwin-Mikke (Konfederacja) – spoza składu Komisji:

Czy mogę mieć pytanie?

Przewodniczący poseł Michał Jach (PiS):

Tak. Za chwilę. Pan poseł Poncyljusz. Tak? Proszę bardzo.

Poseł Paweł Poncyljusz (KO):

Tak. Szczerze mówiąc, te dwa pytania dotyczące łączności w czołgach i radiostacji kierowałem raczej w stronę pana ministra, zdając sobie sprawę, że pan generał akurat w tych kwestiach ma mniej do powiedzenia.

Sekretarz stanu w MON Wojciech Skurkiewicz:

To chyba tym bardziej powinien pan sobie zdawać sprawę z tego, że również panu nie odpowiem na to pytanie. Śledząc pana aktywność, przypuszczam, że pewnie udzielimy jej w formule pisemnej.

Poseł Paweł Poncyljusz (KO):

Trzymam za słowo, panie ministrze. Już mi pan obiecywał pokazać w Kancelarii Tajnej dokumenty dotyczące zbiórki Wojsk Obrony Terytorialnej w dniu, w którym odbywała się wielka manifestacja Strajku Kobiet w Warszawie, ale nie dostałem ich do dzisiaj. Mam nadzieję, że tym razem dostanę wszystko razem, chociażby w Kancelarii Tajnej.

Panie generale, nie wiem, czy uznanie „secret” za „tajne” jest do końca prawidłowe. Rozumiem, że tłumacząc to wprost z języka angielskiego, tak wynika. Ale mamy sytuację, w której pojazdy amerykańskie są w trybie „secret”. Dobrze wiemy, że one nie

są wykonane z żadnej specjalistycznej stali, która powoduje nieprzenikanie sygnału elektromagnetycznego na zewnątrz. Z tego co wiem, cały czas jest problem dostosowania standardu tajności właśnie do tego, jak robią to sojusznicy. A tym bardziej Amerykanie, od których pozyskujemy różnego rodzaju sprzęt z drugiej ręki. Nie mówię, że z demobilu, ale używany. Tam jest protokół „secret", ale pomimo tego nie jest to na przykład stal…

Dyrektor NCBC gen. Karol Molenda:

Już wiem, o co chodzi.

Poseł Paweł Poncyljusz (KO):

To dokończę swoje wystąpienie. Oczywiście za tym idzie duża liczba urządzeń wewnątrz pojazdu, które są bardziej skomplikowane. W przypadku poziomu taktycznego wartość informacji jest często istotna przez pół godziny lub godzinę, bo w tym czasie żołnierz lub pojazd przemieszcza się w inne miejsce. Nawet jeżeli byłby to protokół „zastrzeżone", to prawdopodobnie przez ten czas nikt nie byłby w stanie przez ten czas – biorąc pod uwagę szyfratory – złamać tej informacji, jeżeli byłaby szyfrowana.

I druga rzecz, która wynika z tego, co pan powiedział. Zadaję panu pytanie, zdając sobie sprawę, że pan jako NCBC opiniuje i jest w całym procesie definiowania pewnych parametrów sprzętu czy urządzenia. Dlatego pana o to zapytałem. Zdaję sobie sprawę, że pan jest w grupie tych instytucji wojskowych, które mają nie tylko rolę doradczą. Z tego co wiem, w wielu miejscach jest to rola kluczowa. To znaczy, że jeżeli ktoś z dostawców się z państwem nie porozumie, to tak naprawdę nic nie przechodzi. To też nie jest tak, że jesteście tylko skromnymi krewnymi, którzy siedzą w kąciku. Dziękuję bardzo.

Przewodniczący poseł Michał Jach (PiS):

Dziękuję. Proszę bardzo, pan poseł Korwin-Mikke.

Poseł Janusz Korwin-Mikke (Konfederacja) – spoza składu Komisji:

Panie generale, powiedział pan, że jeżeli coś zostało zaatakowane z terenu szpitala, to nie wiedzieliście, jak odpowiedzieć. Co to znaczy „zaatakowane"? Jak odpowiedzielibyście, gdyby to nie było na przykład ze szpitala, ale na przykład z kantyny wojskowej? Jak odpowiedzielibyście? O co konkretnie tu chodzi?

Przewodniczący poseł Michał Jach (PiS):

Proszę bardzo. Chyba wszystkie pytania były do pana generała.

Dyrektor NCBC gen. Karol Molenda:

Chyba dopiero teraz zrozumiałem sens pytania pana posła Poncyljusza, więc odpowiem jeszcze raz. W ramach porozumień międzynarodowych czy uznania informacji niejawnych „tajne" to jest „secret", a „secret" to jest „tajne". Tak jest w ramach bilateralnego porozumienia zawartego – jak przypuszczam – między rządami Stanów Zjednoczonych i Polski. Tak było to określane. Jeżeli informacja jest „US secret", to ma być traktowana, ma być chroniona tak samo jak nasze narodowe „tajne", bo to jest nasze zobowiązanie pomiędzy dwoma krajami. To jest jedna z tych rzeczy.

Kolejny aspekt. Już teraz wiem, o co panu posłowi chodziło. Amerykanie nie mają ustawy o ochronie informacji niejawnych. To ustawodawca narzucił. Amerykanie nie mają ustawy o ochronie informacji niejawnych. Prosta rzecz. Oni mają risk assessment. Mają analizę ryzyka. I oni określają, że ich służby robią testy penetracyjne, robią analizę ryzyka. Pięknym przykładem tego jest to, że Amerykanie przyjeżdżają, rozkładają swój szyfrator, podłączają go do internetu i mają poziom „US secret". Kiedyś to zobaczyłem, jeszcze w tym nie będąc, i pomyślałem: Boże, to fantastyczne, I have a dream now, chcę tak samo.

Okazuje się, że u nas nie da się tak samo. Nie dlatego, że nie da się tego zrobić pod względem technologicznym, że jesteśmy tutaj – jak pan zauważył – skromnym kuzynem. Nie. Tylko mamy pewne obwarowania. U nas jest ustawa o ochronie informacji niejawnych, która narzuca pewne zobowiązania dotyczące ochrony elektromagnetycznej. Amerykanie bardzo rzadko robią to w ramach risk assessment. Faktycznie, możemy o tym dyskutować. Jako inżynier zakładam, że jest możliwość. Widziałem to. Można odczytać informacje ze strumienia elektromagnetycznego z komputera, z monitora itd. To ist-

nieje. Natomiast ocena ryzyka, że ktoś to zrobi w całym szumie informacyjnym, jest bardzo niska. Dla Amerykanów jest to akceptowalne ryzyko. Ale dla nas, jeżeli mamy ustawę, to zakładamy, że mamy coś tajnego.

Jak pan poseł wskazał, to ma mieć odpowiedni poziom zabezpieczenia urządzenia. Czyli dla przykładu ten szyfrator musi być w odpowiedniej obudowie. Muszą być spełnione pewne warunki bezpieczeństwa tego szyfratora. Dla przykładu ingerencja w szyfrator powoduje skasowanie wszystkich informacji, które są w nim przechowywane, kluczy, itd., itd. W tym momencie faktycznie może dochodzić do takiego scenariusza, że są dwa sojusznicze kraje, ale ich interoperacyjność, czyli umiejętność budowania systemów na tym samym poziomie, jest inna. Ale to nie wynika z tego, że tak chce NCBC czy w przeszłości NCK. Narodowe Centrum Kryptologii, tak jak siły zbrojne i jak – przypuszczam – każdy z nas, działa w granicach obowiązującego prawa i na podstawie obowiązującego prawa.

Jeżeli ustawodawca określił, że mamy ustawę o ochronie informacji niejawnej i mamy jej przestrzegać, to musimy jej przestrzegać. Dobrze wiem, że siły zbrojne występowały z wnioskiem i ta ustawa ma być prawdopodobnie aktualizowana. I to, o czym wspominał pan poseł, czyli te możliwości dla wojsk, dla sił zbrojnych. W moim przekonaniu – być może to jest subiektywna ocena – część tej ustawy została napisana przez urzędników, którzy nie byli w polu. I oni traktują to tak, że jeżeli jest dokument tajny czy system tajny, to mur ma mieć dwa metry, siatka w murze ma być taka i taka strefa. To ma się nijak do sytuacji żołnierza w wozie, dla przykładu w stacji dowodzenia. Ja ich rozumiem.

Przypuszczam, że będzie taki wniosek do państwa. A pewnie będzie to podnoszone w ramach aktualizacji ustawy o ochronie informacji niejawnej. Zdaję chyba sobie sprawę z tego – jeżeli mam dobre informacje – że we wnioskach do ustawy była propozycja, żeby to zmienić. Żeby był większy nacisk na ocenę ryzyka. Żeby był większy nacisk na zarządzanie. Jest wojna i dowódca akredytuje sobie teraz system do poziomu tajnego? Wysyła dokumentację do SKW i przez pół roku czeka na opinię? Przecież to jest wariactwo. Ale tak jest. Panie pośle, to jest wpisane do ustawy. Myślę, że w tej sprawie musimy zrobić bardziej zamknięte spotkanie.

Oczywiście jest zagrożenie. Jeżeli jest to komputer w szpitalu, to nigdy nie wiemy, czy on nie podtrzymuje czyjegoś życia. I to jest to. Załóżmy, że możemy go wyłączyć zdalnie. Czyli na przykład komputer coś robi, atakuje albo zabiera nam informacje. Próbuje zabierać nam informacje. Teoretycznie ci, którzy prowadzą operację, widzą, że ten komputer coś robi. Jeżeli ma podatności, a często ma – bo częstym błędem atakującego jest to, że sam jest otwarty, bo nie wie, jak się zabezpieczyć – to atakujący ma miecz, ale nie ma tarczy. Gdyby były odpowiednie przepisy i można byłoby działać, to odpowiadający na atak – a Francuzi zdefiniowali, że jeżeli jest atak skierowany na siły zbrojne, to mogą one odpowiedzieć adekwatnie do ataku – mogliby w tym przypadku przeprowadzić atak na ten komputer. Jeżeli ten komputer byłby w szpitalu i na przykład podtrzymywał czyjś respirator, który wyłączylibyśmy, to spowodujemy jakieś straty. Gdyby jeszcze druga strona udowodniła, że zrobili to żołnierze, to jest to pewnie najlepszy argument, żeby wypowiadać wojnę albo podjąć inne działania. Nie wiem, czy to by się zakończyło notą dyplomatyczną. Przypuszczam, że żadnej noty by nie było. Kraje dzielą się na te, które przestrzegają prawa, zobowiązań, które mają, i rezolucji ONZ itd., i na takie, które nie o wszystkim pamiętają. Natomiast mi chodzi o przejrzystość, żebym wydając polecenie, wiedział, w jakim zakresie mogę wydać ten rozkaz w dół i co żołnierz może zrealizować w czasie „P”. Nie okłamujmy się. Wojna w cyberprzestrzeni tak naprawdę odbywa się w czasie „P”. Jeżeli gdzieś już wjechałyby czołgi, to z tą cyberprzestrzenią może być różnie. W tym momencie może jej na przykład nie być. Wtedy utrzymywanie wojska, żeby działało w czymś, czego nie ma albo co jest wyłączone, nie do końca jest optymalnym rozwiązaniem.

Przewodniczący poseł Michał Jach (PiS):

I ostatnie pytanie. Pan poseł Poncyljusz.

Poseł Paweł Poncyljusz (KO):

Teraz już do pana ministra, jeżeli pan generał odsyła mnie do Ministerstwa Obrony Narodowej. Panie ministrze, to, co powiedział pan generał, to jest właśnie kwintesencja. Z jednej strony cały czas walczymy o interoperacyjność z naszymi sojusznikami. W technologiach, w tych samych urządzeniach szyfrujących itd. A okazuje się, że pod względem legislacyjnym sami trochę się wyłączamy z takiej interoperacyjności. W związku z tym jest tu pewien absurd. Oczywiście rozumiem, że szyfrator do informacji „secret" musi być tajny i musi być obudowany. Ale szyfrator wstawiony do Humvee – Humvee jako urządzenie, jako nowy Oshkosh, jako wóz dowodzenia czy stacja dowodzenia – nigdy nie będzie w polskich warunkach w kategorii „tajne". Jak szybko Ministerstwo Obrony Narodowej planuje dokonać jakiejś zmiany w tej ustawie, która dotyczyłaby tylko sił zbrojnych? Możliwe, że są jeszcze w Polsce jakieś inne jednostki, podlegające na przykład ministrowi spraw wewnętrznych, które też potrzebują tego typu wyłączeń. Wydaje się, że na poziomie taktycznym ustawienie tego na poziomie „tajne" jest trochę przesadne, biorąc pod uwagę – jak powiedziałem wcześniej – żywotność tej informacji i istotność tej informacji na szczeblu taktycznym.

Sekretarz stanu w MON Wojciech Skurkiewicz:

Panie pośle, jak powiedziałem, pracujemy nad tym. Przygotowujemy takie zmiany, które dotyczą dostępu do informacji niejawnych, a przede wszystkim przetwarzania informacji niejawnych chociażby poza kancelariami i poza stacjonarnymi miejscami, w których to wszystko się odbywa. Zdajemy sobie sprawę, że dzisiejsze przepisy nakładają takie rygory i obostrzenia, które praktycznie są bardzo trudne do zrealizowania. Zabezpieczenia muszą być tak przygotowane, że chociażby w warunkach polowych jest to trudne do przejścia. Stąd zespół, który pracuje nad tymi rozwiązaniami. Mam nadzieję, że lada moment – tylko proszę na mnie nie patrzeć, że to będzie w ciągu tygodnia, miesiąca czy dwóch miesięcy – przygotujemy takie rozwiązania.

Abstrahując od tematyki dzisiejszego posiedzenia, powiem, że w ministerstwie bardzo intensywnie pracujemy nad zmianami legislacyjnymi w wielu aspektach. Jest powołana specjalna komisja kodyfikacyjna, która ma bardzo dużo pracy. Więc 2021 r. będzie rokiem szczególnym, chcemy wszystkie akty prawne, których naprawdę mamy bardzo wiele, traktujące o kwestiach dotyczących obronności skupić w dwóch aktach prawnych, które będą zbierały wiele elementów rozsianych w różnych miejscach. Chcemy też ujednolicić kwestie dotyczące wielu rozporządzeń. Rozporządzeń, które choć obowiązujące, nie są adekwatne do obecnej sytuacji, jeżeli chodzi o obronność. Chcemy również ujednolicić kwestie decyzji, które na przestrzeni lat zostały tak namnożone, jeżeli chodzi o resort obrony narodowej, że nie są znane. Kiedyś zadałem dowódcom pytanie, czy znają chociaż 10% decyzji, które obowiązują w Wojsku Polskim czy w Ministerstwie Obrony Narodowej – bo to już nie są dziesiątki czy setki, tylko tysiące decyzji, które dziś obowiązują.

Podjęliśmy się tytanicznej pracy. Naprawdę to jest tytaniczna praca. To jest kilkunastoosobowy zespół, któremu przewodzę. Przygotowuje on właśnie takie rozwiązania. Myślę, że 2021 r. będzie bardzo ważny, przynajmniej w zakresie legislacyjnym. Kwestie dostępu i ochrony informacji niejawnych to są rzeczy, które musimy przepracować. Dlatego że – jak tu powiedziano – relacje sojusznicze są szczególnie istotne. I to musi być ujednolicone.

Przewodniczący poseł Michał Jach (PiS):

Dziękuję, panie ministrze. Dziękuję również, panie generale. Dzisiaj było wyjątkowo interesująco. To chyba wszyscy przyznają. Proszę państwa, jeżeli nie ma żadnych uwag, to dziękuję państwu. I zamykam posiedzenie Komisji Obrony Narodowej. Ale jeszcze przed zamknięciem przypominam, że informacja, o której wspominał pan generał Molenda, znajduje się w sekretariacie Komisji Obrony Narodowej. Jeśli ktoś chce się z nią zapoznać, zapraszam do pokoju 201A w starym domu poselskim.

Zamykam posiedzenie.